Establishing effective public-private partnerships on countering the financing of terrorism

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

CTED Analytical Brief
December 2023

TABLE OF CONTENTS

Copyright © United Nations Security Council
Counter-Terrorism Committee Executive Directorate.

Photos: iStock.com/metamorworks
iStock.com/matdesign24

December 2023

BACKGROUND AND METHODOLOGY

The present Analytical Brief was prepared by the Counter-Terrorism Committee Executive Directorate (CTED) in accordance with resolution 2395 (2017), in which the Security Council directs CTED to conduct analytical work on emerging issues, trends, and developments and to make its analytical products available throughout the United Nations system. More recently, in resolution 2617 (2021), the Council reiterated the essential role of CTED within the United Nations to identify and assess issues, trends, and developments relating to the implementation of relevant counter-terrorism resolutions, including 2462 (2019) on countering the financing of terrorism (CFT).

CTED Analytical Briefs aim to provide the Security Council Counter-Terrorism Committee, United Nations agencies, and policymakers with a concise analysis of specific issues, trends, and developments, as identified through CTED's engagement with Member States on their implementation of the relevant Council resolutions. They also include data gathered by CTED, including through engagement with its United Nations partners; international, regional, and subregional organizations; civil society organizations (CSOs); and members of the CTED Global Research Network (GRN).

The present Analytical Brief is based on information collected through CTED's engagement with Member States, in particular assessment visits conducted by CTED on behalf of the Counter-Terrorism Committee, which has also been analysed and reflected in public reports on gaps in implementing key CFT provisions of the Security Council resolutions.[1] CTED's engagement has also included outreach to United Nations partners, international and regional organizations, including the Financial Action Task Force (FATF) and its Global Network,[2] as well as to CSOs and GRN and private sector entities,[3] and participation in relevant international and regional events. For this Analytical Brief, CTED also conducted a number of consultations with experts from States that have instituted public-private partnerships (PPPs), including the French Financial Investigation Unit (TRACFIN); the Federal Police Office of Germany Counter-Terrorism Division, in collaboration with the Max Planck Institute; the Terrorism Financing (TF) Taskforce under

[1] CTED, "Thematic summary assessment of gaps in implementing key countering the financing of terrorism provisions of the Security Council resolutions", December 2022, available at www.un.org/securitycouncil/ctc/content/thematic-summary-assessment-gaps-implementing-key-countering-financing-terrorism-provisions.

[2] In addition to the annual Private Sector Consultative Forum, FATF has a standing practice to consult with the private sector in the context of its analytical trends reports and/or policy guidance development. As part of the relevant project teams, CTED also has had access to the feedback received.

[3] E.g., CTED-led technical sessions on "Threats and opportunities related to new payment technologies and fundraising methods" organized in preparation for the Committee's Special Meeting in New Delhi (September 2022); CTED consultations for a set of non-binding guiding principles on "Countering the use of new and emerging technologies for terrorist purposes: threats and opportunities related to new payment technologies and fundraising methods", May 2023.

the Financial Expertise Centre (FEC) in the the Kingdom of the Netherlands; the Malaysia Financial Intelligence Network; and Western Union (South Africa).

Recognizing the need to better understand the effectiveness and any potential unintended consequences of CFT PPPs, as well as to track new developments on the use of new and emerging technologies to enhance the effective implementation of anti-money-laundering (AML)/CFT measures, CTED is committed to pursuing its efforts and engagements in this area.

OVERVIEW

Both the Security Council and the Counter-Terrorism Committee encourage national authorities to establish partnerships with the private sector, including financial institutions, the financial technology industry (fintech), and Internet and social media companies, in particular with regard to the effective implementation of reporting and disclosure requirements, the use and sharing of relevant financial information from the private sector, and the sharing of information on the evolution of trends, sources and methods of the financing of terrorism.[4]

As reflected across a number of FATF recommendations and Immediate Outcomes, it is crucial that information concerning financial activity with possible links to crime and terrorism be shared in a timely and effective manner between and with the public and private sectors. Appropriate information-sharing can allow all relevant stakeholders to make better use of available resources and exploit new technologies and business models to develop innovative techniques to address money-laundering and terrorist financing.[5] Given the large array of legal and operational challenges to sharing information between the public and private sectors, FATF issued dedicated guidance in this regard, highlighting, inter alia, that an effective two-way relationship between the public and private sectors can be achieved if there are appropriate mechanisms for sharing strategic, operational, tactical and targeted information by law enforcement with the private sector.[6]

The private sector, including financial institutions and designated non-financial businesses and professions, plays a vital role in CFT. Within the private sector there are reporting entities obligated under AML/CFT frameworks, with a legal duty to transmit information on suspicious activities to financial intelligence units (FIUs) and/or law

[4] Security Council resolution 2462 (2019), para. 22; Delhi Declaration on Countering the Use of New and Emerging Technologies for Terrorist Purposes, October 2022, paras. 15 and 25.
[5] FATF, *Guidance on Private Sector Information Sharing*, (Paris, 2017), available at www.fatf-gafi.org/en/publications/Fatfgeneral/Guidance-information-sharing.html.
[6] FATF, *Guidance on Private Sector Information Sharing*, (Paris, 2017), p. 27, available at www.fatf-gafi.org/en/publications/Fatfgeneral/Guidance-information-sharing.html.

enforcement agencies. This information is then analysed and used by authorities to proactively prevent, detect, and disrupt terrorism-financing offences. Such information is also essential for authorities to gain a more comprehensive understanding of current and emerging terrorism-financing threats and trends.

While large banks have traditionally been the major providers of information reported under AML/CFT frameworks, an increasing number of fintech, Internet, and social networking services and key economic sectors like those involved in natural resources exploitation, extraction and mining, pharmaceuticals, real estate and construction, which may not be reporting entities in all Member States, have also become an effective, but often underestimated, source for detecting the movements of funds belonging or destined to terrorists and terrorist groups. The appropriate use of the information they can generate can contribute to better identification of terrorist risks, tracing of assets, and mapping of terrorist-related transactions.

In several expert meetings in which CTED participated,[7] some fundraising platform companies shared their insights on community engagement, which is critical for understanding clients and their networks. Social media companies and other non-financial online services also have a role in monitoring fundraising patterns and financial communications, for example knowing their users, while payment service providers have the necessary information to know their networks. As a result, researchers and private sector partners have highlighted the need for cooperation and coherence in regulating financial institutions (which are already subject to AML/CFT controls), crowdfunding sites and social media (to which it could be advisable to apply know-your-client (KYC) and client due diligence (CDD) requirements in relation to fundraisers) as stakeholders that cohabit the same process and possess complementary information. Non-profit organizations and intermediary organizations providing crowdfunding services through dedicated platforms, as well as social media and messaging apps, acknowledge that they face challenges in preventing and detecting the abuse of their services for terrorism financing. Investigative authorities and prosecutors face similar challenges as a result of the complexity and pseudonymity of transactions.[8]

The rapid evolution of financial technologies has made it challenging for authorities to rely solely on compliance with AML/CFT requirements, in particular suspicious transaction reports (STRs). Furthermore, the nature of terrorism financing, which can involve low-value transactions that fall below monitoring or reporting thresholds, and in which various means can be employed to avoid detection and maintain anonymity, has

[7] See for example FATF Joint Expert Meeting (April 2023, New Delhi); Seminar on Countering Terrorist Financing held under the Spanish presidency of the Council of the European Union (September 2023, Madrid).
[8] For example, see FATF, *Crowdfunding for Terrorism Financing*, (Paris, 2023), available at www.fatf-gafi.org/en/publications/Methodsandtrends/crowdfunding-for-terrorism-financing.html ; and Asia-Pacific Group on Money Laundering (APG) and Middle East and North Africa Financial Action Task Force (MENAFATF), "Social media and terrorism financing", January 2019, available at www.menafatf.org/sites/default/files/Newsletter/FINAL-TM-SF-en.pdf.

also increased the need for the private sector to receive more guidance from FIUs, law enforcement, and other authorities regarding terrorism-financing techniques, trends and corresponding red flag indicators. In this regard, PPPs are an opportunity to enhance the private sector's capacity to mitigate high-risk activities and hence better support authorities in preventing and detecting terrorism financing.

While governments tend to expect the private sector to self-police, adequate frameworks for doing so are often missing. To avoid risk, the private sector may over-comply, leading to de-risking practices, including de-platforming and denial of other services, and there appears to be little to no reaction from the public sector in this regard. In addition to the resulting discrimination, potential for marginalization and breaches of human rights, such practices represent missed opportunities to collect information on suspected individuals and networks, potentially pushing them to operate on less accessible platforms (including private chats). Inversely, setting frameworks in tandem allows the private sector and regulators to collaboratively identify risks and pilot a regulatory framework and working arrangements on mutually understandable terms.

Furthermore, the Security Council called for 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. Indeed, and as highlighted by the work of FATF, new technologies also have the potential to make AML/CFT measures in both the public and private sectors faster, cheaper and more effective. When used responsibly and proportionally, technology can facilitate data collection, processing and analysis and help actors to identify and manage terrorism-financing risks more effectively and closer to real time. This is another important area where robust PPPs are critical.

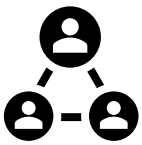
A multi-stakeholder approach, i.e., one that involves a range of relevant public authorities, the private sector, civil society and academia, is key at all stages of designing and implementing CFT measures: from risk assessment, to developing and implementing risk-based measures, to assessing their effectiveness and any adverse or unintended impacts.

In the context of its 2022 thematic summary assessment of gaps and areas requiring more action to implement key CFT provisions of the relevant Council resolutions,[9] CTED noted that most of the States evaluated during the reporting period lacked robust PPPs to share information, understand evolving trends, including to better understand the nexus between terrorism and organized crime, increase knowledge and skills of relevant experts, and strengthen the integrity of the financial sector.

[9] CTED, "Thematic summary assessment of gaps in implementing key countering the financing of terrorism provisions of Security Council resolutions", 2022, available at www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/cted_2022_cft_gaps_assessment_final.pdf.

The current Analytical Brief underscores the need for States to allocate sufficient resources to both public and private sector stakeholders and to continue to strengthen collaboration frameworks for the competent national authorities (not only FIUs but also any other agencies playing a role in CFT, such as law enforcement and customs) and the private sector to effectively combat terrorism financing, while ensuring full respect for international law, including international human rights law, international humanitarian law and international refugee law. Such frameworks should include clear provisions on what information can and cannot be shared and under which circumstances and with which stakeholders, as well as oversight and accountability mechanisms to safeguard the rights to privacy and data protection.

FRAMEWORKS FOR PUBLIC-PRIVATE PARTNERSHIPS



As terrorist financers exploit various tools across and within private sector industries, some Member States recognize that PPPs are a way for private sector institutions, which are often unable to share essential information with each other, to warn the industry/sector about how terrorist financers are exploiting products and services. PPPs can be instruments that provide opportunities for proactive sharing of relevant information, enabling the early identification of threats. They may also be mechanisms to address information exchange that requires immediate and urgent action.

Partnering with the private sector has the potential to enhance information-sharing frameworks, thereby fostering a more results-driven implementation of CFT measures. In particular, in countering the financing of terrorism, timeliness in information-sharing is critical. As such, properly established PPPs bring an added layer of structured and trusted cooperation and enhanced information-exchange between the private and public sectors, with the benefits of two-way information exchange, the sharing of relevant information, including early warnings, in real time, alerting each other to new trends and supporting each other in addressing such trends effectively and proportionally to the real risks.

The private sector is equipped with data and the necessary technology for analytics while law enforcement holds the expertise on countering threats. PPPs have the potential to provide an intersection between the two. Responsible use of technology and data, including blockchain and artificial intelligence, can advance operational and tactical analysis, map terrorist financial networks, and track and report suspicious activity.

However, there is also a certain amount of asymmetry and misalignment of goals.[10] Private sector entities are mostly focused on establishing processes and procedures to

[10] Cf. Patrick Hardouin, "Banks governance and public-private partnership in preventing and confronting organized crime, corruption and terrorism financing", *Journal of Financial Crime*; Vol. 16, Issue 3, (July 2009), pp. 199-209.

comply with legal and regulatory provisions and to avoid risks and potential reputational damage. As a result, the private sector will tend to limit information-sharing with the public sector to what is strictly required by law. Law enforcement, on the other hand, is usually rather sensitive on terrorism matters and sometimes legally prevented from exchanging information with private sector entities. In view of the classified nature of the information held by the public sector, the private sector is often ''deprived'' of information that could assist it in making informed decisions on what can be proactively and beneficially shared with the public sector.

As noted by FATF, through such partnerships, information is shared across law enforcement, FIUs, and vetted participants from the private sector, as well as international partners in some cases. An established process of data-mining, operational analysis and scanning by the private sector, with reciprocal exchange with the public sector, facilitates a more comprehensive view of transactions and customers' behaviour to fill potential intelligence gaps. Initiatives can also be steered within the private sector, through, for example, exchange of information within the same group of financial entities, domestic and foreign branches, or an interbank forum to share information on recent crime trends, modus operandi and typologies among participants with the support and collaboration of law enforcement and supervisory authorities. In such cases, safe harbours can carve out specific legal protections to enable information-sharing between financial institutions for AML/CFT purposes.[11]

CTED assessments indicate that Member States face challenges in institutionalizing partnerships with the private sector on financial information-sharing and more specifically in the context of CFT. Once established, these partnerships can take diverse forms, not all of which are fully effective or sufficiently safeguarded.

With information exchanged on a real-time basis, multi-stakeholder PPPs allow for the design of more effective and comprehensive investigation strategies, as they enable public sector authorities to work with the private sector in tracking, mapping, and identifying terrorist networks more proactively. This is particularly useful in situations where different sectors are involved and not all of them are subject to the same regulations or have access to the same information. For example, a fundraising campaign facilitated through crowdfunding platforms or social media can also involve formal financial sector and/or virtual asset service providers, and the non-profit sector as a beneficiary. Each of these stakeholders operate under different regulatory frameworks, implement different checks and controls (if at all), and only a few of them would be obligated to report any suspicious information to the relevant authorities. In addition, the ones that report the information may only have certain elements they are obliged to trace, while other important information stays with stakeholders who do not report or share it.

[11] FATF, *Guidance on Private Sector Information Sharing*, (Paris, 2017), available at www.fatf-gafi.org/en/publications/Fatfgeneral/Guidance-information-sharing.html .

On the receiving end, the authorities will not have all the information needed to analyse the full picture.

Establishing a clear legal basis for the sharing of information between public and private sectors is essential not only to allow for those exchanges to take place but also to define the exact criteria and purposes for which information may be shared and the entities with which it can be shared. In addition, frameworks and procedures for feedback mechanisms between law enforcement, financial intelligence units and reporting entities from relevant sectors can help to improve the quality of reports and financial intelligence products, as well as to support trends monitoring and strategic analysis. 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), developed data-sharing frameworks and protocols not only facilitate information exchange between the different entities involved in CFT but also ensure the safeguarding of human rights, including the right to privacy and data protection. Defining oversight mechanisms under such frameworks also ensures that relevant PPPs adhere to data protection or privacy obligations under national legislation as well as applicable international frameworks.

The landscape of PPPs for sharing financial information is characterized by a wide diversity, with most PPPs having a broader scope beyond just targeting CFT. It is important to grasp these nuances since there is no single specific model underlying the term “PPPs”. In practice, it encompasses various mechanisms of information exchange between the public and private sectors, whether occurring within an explicitly labelled PPP or through other modalities.

STRATEGIC INFORMATION SHARING

Some forms of cooperation between national authorities and the private sector are referred to as PPPs, but in essence, are more strategic in nature and primarily serve to co-develop typologies and knowledge products covering threats and relevant risk indicators. Typically, these products do not contain confidential or identifying information about specific suspects and entities. For example, in France TRACFIN may issue “calls for vigilance” disseminated to reporting entities. The aim is to help the implementation of their risk-based approaches by drawing their attention to a particular situation. In 2019, TRACFIN issued eleven “calls for vigilance” relating to terrorist financing. This form of sensitization can focus on targeted vulnerable sectors but can be useful for the entire industry as well. Canada’s FIU, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), provides another illustration of awareness-raising on subject-specific dissemination of information. FINTRAC’s strategic intelligence products provide analytical perspectives on the nature,

scope and threats posed by terrorism financing for specific sectors, key patterns in suspicious transactions associated with terrorism and violent extremism acts on the basis of xenophobia, racism and other forms of intolerance, or in the name of religion or belief, and indicators of terrorist financing activity in relation to foreign terrorist fighters.

OPERATIONAL PARTNERSHIPS

Other forms of PPPs have been set up to be more operational in nature, allowing for exchange of information on incidents, actors and entities and their financial operations. Those PPPs involve the sharing of more sensitive information that can be used in financial intelligence and investigative operations and where the private sector not only ensures compliance with financial crime regulation but becomes a contributor to investigative efforts.[12] Concurrently, it assists the private sector in improving the effectiveness of customer due diligence[13] and identifying higher risk customers.[14] Operational PPPs do not necessarily include several entities from the private sector but instead earmark more vulnerable and key institutions/sectors to develop information-exchange mechanisms with a more targeted approach. The most well-known examples are the Joint Money-laundering Intelligence Taskforce of the United Kingdom of Great Britain and Northern Ireland, which has resulted in a number of successful investigative operations, and the United States Department of the Treasury's Financial Crimes Enforcement Network. More recently, the Kingdom of the Netherlands' Financial Intelligence Unit has developed a rapprochement with banks to work collaboratively on an array of reports and STRs. The Malaysia Financial Intelligence Network also includes tactical objectives, such as the sharing of information on specific cases for further review by reporting institutions.[15]

[12] For some examples, see Eurasian Group on Combating Money Laundering and Financing of Terrorism, "Legalization (laundering) of the proceeds of cybercrime, as well as financing of terrorism from the said offence, including through the use of electronic money or virtual assets and the infrastructure of their providers (2022)", pp. 10–11, available at https://eurasiangroup.org/files/uploads/files/other_docs/WGTYP_(2022)_12_rev_1_eng.pdf.
[13] Caribbean Financial Action Task Force Research Desk, "The importance of public private partnerships in AML/CFT", 2022, p. 5.
[14] FATF, *Guidance on Private Sector Information Sharing*, (Paris, 2017), p. 13, available at www.fatf-gafi.org/en/publications/Fatfgeneral/Guidance-information-sharing.html.
[15] This has led to the arrest, prosecution and deportation of 22 individuals for their suspected involvement in terrorism and proliferation financing activities in Malaysia.

MODALITY OF PARTNERSHIPS

As part of executing their plans, some PPPs have established dedicated workspaces with access restricted to nominated personnel or key participants only, enabling real-time collaboration in cases or operations, as seen, for example, in the Latvia Cooperation Coordination Group. On the other hand, some prioritize the development of dedicated communication platforms for information exchange, exemplified by the Singapore Anti-money-laundering and Countering the Financing of Terrorism Industry Partnership. Regarding governance, most PPPs are led by competent authorities, while others have oversight mechanisms where both government and industry representatives oversee operations and set the agenda for future work, as observed in the Australian Fintel Alliance, which successfully provided intelligence to the Federal Police on persons of interest which led to a disrupted terrorist attack.[16]

Effective cooperation between the two sectors on a more targeted basis has also proved possible. For instance, the French FIU (TRACFIN) has established bilateral information exchange protocols with selected private sector entities and, in 2019, launched a special committee for combating terrorism financing to formalize information exchange between TRACFIN and obligated entities.

Certain PPPs have been established at the supranational level, some with a more permanent structure, such as the European Union Agency for Law Enforcement Cooperation (Europol) with its Financial Intelligence Public-Private Partnership, established in 2017, while others are more project-oriented, developing best practices, capacity-building and networking initiatives among public and private actors. The BeCaNet initiative (best practice, capacity building and networking initiative among public and private actors against terrorism financing) is a two-year effort directed by the German Federal Criminal Police in collaboration with authorities from France, Spain, and the United States to build networks between private and public stakeholders to counter terrorism financing.

On a regional basis, FATF-style regional bodies have launched initiatives for closer collaboration with the private sector. A notable example is a series of consultative forums held by the Eurasian Group on Combating Money Laundering and Financing of Terrorism since 2006, with the aim of improving public-private sector engagement to enhance AML/CFT systems and the exchange of guidelines and feedback between both sectors and addressing emerging issues related to new payment methods. This Consultative

[16] FATF, *Partnering in the Fight Against Financial Crime: Data Protection, Technology and Private Sector Information Sharing*, (Paris, 2022), p. 64, available at www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf.coredownload.pdf. See also Asian Development Bank (ADB), ADB Briefs on "Financial crimes compliance: the power of partnerships", No. 180, July 2021, available at https://www.adb.org/publications/financial-crimes-compliance-power-partnerships.

Forum allows for the formulation of recommendations on mutually understandable terms. The Alliance for Financial Inclusion under the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG) conducted a Public and Private Sector Surveys Report on Financial Integrity and Financial Inclusion Frameworks and Compliance Practices in 2013 and also assessed the level of communication with the private sector and the impact of de-risking. Similarly, the 2020 report on the assessment of counter terrorist financing activities of the Intergovernmental Action Group against Money-Laundering in West Africa (GIABA) identified gaps in the reporting of suspicious activity by the private sector and included a series of recommendations.

ADDRESSING GAPS AND CHALLENGES IDENTIFIED IN PPP FRAMEWORKS

LACK OF RESOURCES AND CAPACITY

One of the common challenges to effective PPPs on AML/CFT matters is inadequate investments in the material, financial and human resources both in private sector and governmental authorities, including FIUs.[17]

In this regard, Governments should invest more in AML/CFT-related resources and promote effective coordination of targeted capacity-building activities to build a pool of national expertise.[18] Another good practice is the reorganization of relevant services to optimize human resources and track down a maximum number of cases involving the interests of the State.[19] Furthermore, taking into account and assessing the effectiveness of information flow through PPPs, both the public and private sectors could capitalize on the cost-benefit of such partnerships by, for example, designating dedicated focal points within their specialized units to coordinate on specific areas. The added benefit of pooling focal points is the rapport and

[17] Highlighted in CTED's engagements with relevant stakeholders. The challenge is also mentioned, for example, in *GIABA Research and Documentation Report, An Assessment of the Challenges Associated with the Investigation, Prosecution and Adjudication of Money Laundering and Terrorist Financing in West Africa, Assessment Report*, (Dakar, 2021), para. 188, available at www.giaba.org/media/f/1302_An%20Assessment%20of%20Challenges.pdf ; ESAAMLG, *Report on Money Laundering through the Securities Market Industry in the ESAAMLG Region*, (2015), pp. 56–58, available at https://www.esaamlg.org/reports/Report%20on%20ML%20&%20TF%20through%20the%20Securities%20Market%20Industry%20in%20the%20ESAAMLG%20Region..pdf .

[18] Ibid., p. 54; and ibid., p. 58.

[19] *GIABA Research and Documentation Report, An Assessment of the Challenges Associated with the Investigation, Prosecution and Adjudication of Money Laundering and Terrorist Financing in West Africa, Assessment Report*, (Dakar, 2021), p. 31, available at www.giaba.org/media/f/1302_An%20Assessment%20of%20Challenges.pdf .

trust built between the collaborating points of contact, which in turn ensures the protection of confidentiality of information exchanged.

LIMITING THE SCOPE OF PPPS TO TRADITIONAL FINANCIAL INSTITUTIONS

In the context of the increasing number of fintech companies and decentralized financial services, customers are increasingly using varied forms of financial products and services in place of traditional banking. As a consequence, customer data are becoming more dispersed, making it more challenging to obtain terrorism-financing insights based on data from a single institution. Different terrorist groups have been reported to exploit a multiplicity of methods, including cross-border transportation of cash and hawala-type transfers, in combination with new and emerging payment methods (for example, prepaid cards, mobile payment systems, virtual and online exchanges and wallets, and virtual assets). Partnering with each such sector involves its own challenges.

Against this backdrop, the more established PPPs primarily focus on collaborating with financial institutions, especially retail banks, and consist of a limited number of private sector members compared to the entities regulated for AML/CFT purposes. Taking this into consideration, some Member States are developing PPPs based on pilot initiatives, with the intention of expanding the operational scope and acquiring more resources in the future to include more members. As an example, in the Kingdom of the Netherlands, the Terrorist Financing Task Force, primarily composed of the largest banks in the country, is exploring the possibility of involving other private sector members. Another example is the 2022 South African Anti-Money Laundering Integrated Task Force initiative to disrupt financial crimes connected to the illegal wildlife trade by partnering with United for Wildlife.

When asked about private sector representation in PPPs, some experts have emphasized the importance of trust, which is dependent on a manageable size to maintain the confidentiality of the intelligence shared and to enable effective decision-making. However, this may conflict with the need for flexibility and dynamism, as key actors can swiftly change and the rapid changes in the way new financial technologies are exploited by terrorists. With regard to collaboration with fintech, Internet, and social networking services in CFT efforts, Member States, particularly FIUs, primarily reported the mitigation of terrorism-financing risks through the issuance of typologies and risk indicators for awareness-raising purposes. For instance, in France, TRACFIN utilizes social media to share typologies and practical cases and also organizes webinars and seminars related to AML/CFT. A notable example is its latest video demonstrating the use of anonymous vouchers converted into virtual assets by transnational terrorist networks employing a

combination of conventional transaction systems, such as hawala, with a sophisticated array of tools and methods involving new technologies.

While PPPs have enhanced information-sharing mechanisms, as part of States' AML/CFT efforts, current partnerships might not sufficiently focus on pertinent information in key and particularly vulnerable areas. CFT, specifically, requires proactive cooperation with vulnerable sectors not limited to cooperation between traditional financial sectors and FIUs/law enforcement agencies. A few examples of vulnerable sectors include those operating new payment methods, money value transfer services, entities trading in natural resources, in particular in the gold sector, and the antiquities and art markets, as well as companies operating in free trade zones. The aim would be to develop targeted cooperation mechanisms between key private sector areas with higher terrorism-financing incidences and the corresponding public sector.

The selection to and prioritization of private sector members for a PPP should be guided by an up-to-date terrorism-financing national risk assessment, backed by a comprehensive and effective strategy to combat terrorist financing. For example, as highlighted in TRACFIN's latest activity report, half of the STRs from the crowdfunding platforms re related to terrorism financing.[20]

UNCLEAR LEGAL FRAMEWORKS

While States may have laws requiring obliged entities to report information when a suspicion of crime or terrorism financing arises, this is only one way, CFT communications happen and does not cover all the practices, including information shared on a voluntary basis. Collaboration is challenging given the bans in legislation, including data privacy laws, which overall, impede the ability of law enforcement to obtain information needed for investigations.[21] Some research studies have explored the extent to which informal exchanges, not covered by the law, are conducted through direct relationships, in which the information shared is on a need-to-know basis, independently of any standing agreement. This is also facilitated when personnel from the public sector move to the private sector and are able to more easily establish individual contact points. However, the role of public-private information-sharing in supporting ongoing

[20] For more information on practices and challenges to address the use of crowdfunding for terrorism financing, see TRACFIN's latest activity report, *AML/CFT: Reporting Entities Activity 2022 Review*, (2022), available at www.economie.gouv.fr/files/2023-06/TRACFIN_2022_EN_Web.pdf ; and FATF, *Crowdfunding for Terrorism Financing*, (Paris, 2023), available at www.fatf-gafi.org/publications/Methodsandtrends/crowdfunding-for-terrorism-financing.html .

[21] See *GIABA Research and Documentation Report, An Assessment of the Challenges Associated with the Investigation, Prosecution and Adjudication of Money Laundering and Terrorist Financing in West Africa, Assessment Report*, (Dakar, 2021), p, 8, available at www.giaba.org/media/f/1302_An%20Assessment%20of%20Challenges.pdf .

investigations raises questions about the interplay between criminal procedures and AML/CFT laws. Informal practices for information-sharing in criminal investigations, facilitated through PPPs, can lead to significant challenges to the admissibility of information as evidence in criminal proceedings and lack of clarity about the role and legal implications for reporting institutions which, in some instances, can compound the lack of trust and result in impediments to disclosures. In an attempt to bring more certainty, some PPPs consult with the private sector before an action is taken to ensure they have a common understanding and approach. Such methods could help to avoid unintended consequences. For example, obliged entities can be informed upfront that they should be strictly prohibited from sharing the risk notification and its content with third parties without prior authorization, and they should not take any action that could jeopardize any investigation.

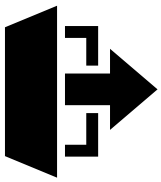
In this regard, the widespread use of informal practices as opportunities to cooperate with the private sector underscores the need for focused and clearer legal frameworks, which also take into account the rights and obligations of the private sector, including safeguards for the protection of the information and the source.

Gaps in legal frameworks also affect social media companies and certain crowdfunding platforms that are not reporting entities but can nevertheless be exploited by terrorists to raise and move funds. Through outreach and awareness-raising initiatives, PPPs can help to ensure that the CFT efforts of social media companies and the crowdfunding industry are informed and effective, which affords them a layer of protection in their activities and equips them with tools to be aware of risk indicators and ultimately mitigate and/or report suspicious activity. The APG/MENAFATF report “Social media and terrorism financing ” provides case studies and a set of comprehensive recommendations in this regard.[22.]

As FATF has noted, a national CFT strategy, based on a thorough and up-to-date risk assessment, reinforces legal frameworks and provides a solid foundation for operational cooperation between relevant agencies and the private sector, especially with respect to new and evolving financial technologies, which pose a shared challenge for Member States in detecting patterns of suspicious activity and conducting investigations.

[22] Available at www.menafatf.org/sites/default/files/Newsletter/FINAL-TM-SF-en.pdf .

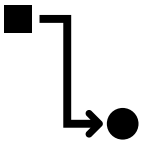
ONE-WAY COMMUNICATION AND LIMITATIONS ON FEEDBACK AND GUIDANCE



In many States, PPPs are limited to one-way communication channels where information is provided or requested on an ad hoc basis, without subsequent follow-up or regular feedback, and therefore these communications fall short of their full potential. Feedback is crucial to better evaluate the utility of the provided information, improve its quality or the focus of future communications, and to ensure a trusted and ongoing dialogue overall. Guidance should be targeted to remaining gaps in knowledge or implementation. Burdens in collecting, and most importantly, processing the vast amount of financial data (including, for example, publicly available virtual asset transaction trails) should be shared between both sectors.

Effective PPPs require an understanding of operational and transactional realities and a focus on sharing and pursuing actionable information. Under the Australia and New Zealand Banking Group Limited initiative[23] and the Fintel Alliance project led by the Australian Reporting and Analysis Centre, more than 160 million transaction reports are received annually and transformed into actionable intelligence to support investigations.[24] Understanding trends requires that law enforcement be familiar with the realities and practicalities of financial transactions and that the private sector be aware of patterns of TF activity. It is imperative to increase the knowledge and skills of relevant experts at both ends of the communication. For example the private sector can be guided on the elimination of bias and faulty data in detection models, including through human feedback loops, in the most effective and human rights-compliant way. Novel sectors like new payment service providers and digital and decentralized finance experts require specific attention in this regard.

UNINTENDED CONSEQUENCES, INCLUDING IMPACT ON HUMAN RIGHTS



Member States with advanced PPPs have established legal frameworks, which vary according to the many possible configurations of information-sharing methods for the private and public sectors and regulate the purposes and means of exchanging information, including processing of personal data. However, States which rely on informal cooperation or weak PPPs may not adopt adequate legal measures to ensure that PPPs adhere to the

[23] This initiative has a presence in 12 countries across the Pacific.
[24] ADB, Brief on "Financial crimes compliance: the power of partnerships", No. 180, July 2021, available at www.adb.org/publications/financial-crimes-compliance-power-partnerships.

right to privacy, data privacy, and data protection principles in accordance with international human rights standards.

PPPs necessarily must involve designing data systems and processes which provide access to and analysis of a wealth of information, often comprising sensitive information, which may result in human rights breaches if disclosed in an arbitrary and unlawful manner. New technologies have further made information exchange more potent. Data protection rules and the protection of the source of the information continue to be challenging, which, in the case of criminal proceedings initiated within the framework of PPPs, can profoundly affect customers and the private entity. The private sector, bound by data protection laws, is also required to respect human rights.[25] Without proper safeguards, public-private information-sharing can lead to bias and racial, political or religious profiling.[26] In that sense, while balancing the demands of efficient information flow, law enforcement and FIUs need to be cautious of what they request from the private sector and need to provide clarity and concrete guidance to avoid miscommunications or the flow of unnecessary information.

Counter-terrorism measures allow States to implement certain restrictions on general data protection principles when necessary and proportionate for the purpose of preventing, investigating, detecting, or prosecuting criminal offences, including terrorism, and safeguarding against threats to public security. These processes may carry inadequate judicial oversight, transparency and remedies, in case of breaches. As noted above, vague and ambiguous legal frameworks can lead the private sector to adopt a reactive approach and over-comply to avoid reputational risks or the threat of legal action. Uncertainty and lack of clarity can inadvertently result in undue interference with the right to privacy and have other negative impacts on freedoms of opinion, expression, association, and religion or belief.[27] For example, when authorities have the ability to influence the private sector's search algorithms, the "indirect" processing of personal or strategic data by authorities carry risks of misuse.

There needs to be consensus in light of constitutional and/or other national law of what is possible in data-sharing. There is a lot of jurisprudence on data protection, but the impact on AML/CFT information exchange is not yet fully understood. As PPPs become a more generalized tool in AML/CFT frameworks, the establishment of regulations and policies that clearly define, with sufficient precision, the permissible grounds, prerequisites, and authorization procedures governing the collection or monitoring of

[25] Guiding Principles on Business and Human Rights, Implementing the United Nations "Protect, Respect and Remedy" framework, 2011, available at: https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf

26 Benjamin Vogel, "Public- private partnerships in the fight against the financing of terrorism", Department of Criminal Law, Max Planck Institute for the study of crime, security and law, 2022. Available at https://csl.mpg.de/en/projects/fight-financing-terrorism.

[27] Nadezhda Purtova, "Between the GDPR and the police directive: navigating through the maze of information sharing in public–private partnerships", 2018.

financial data or information, together with safeguards, will contribute to strengthening the legitimacy of PPPs and the effectiveness of CFT measures.[28]

In such a process, Member States need to ensure that data-sharing frameworks, protocols and oversight mechanisms facilitate CFT information exchange while safeguarding human rights, including the right to privacy and data protection under national legislation, principles of non-discrimination and applicable international frameworks. The private sector is encouraged to use PPPs as a platform to manage and mitigate risks and avoid unduly limiting access to financial services or delaying transactions. Both sectors should synchronize, with a shared approach and understanding.

Despite significant efforts to prevent CFT measures from leading obliged entities to de-risk, with the associated challenges to accessing financial services, such entities can still impose undue restrictions and controls on the activities of their clients and discontinue relationships with customers based solely on a perception of risk.[29] Initial suspicions of criminal justice authorities or FIUs are sometimes based on unverified information and suspicions may later be proved to be unfounded, and their limitations on suspects' rights are usually bound by procedural safeguards. Private sector actors may be reactive and use shared information to close accounts or terminate relations with clients for fear of enforcement actions by AML/CFT supervisors and/or reputational risks.

Such actions taken by private sector entities within a PPP may profoundly impact customers and the private entity's reputation. And, as these reactions occur as a result of information shared within the context of a PPP, it is difficult for competent authorities not to share responsibility. Hence, PPPs need to carefully assess the balance between effective information-sharing and safeguards against potential harm.[30]

On the other hand, partnerships with the private sector should also present opportunities to promote the meaningful involvement of civil society in ensuring that such partnerships do not infringe upon financial inclusion and civic space, including with respect to a chilling effect on legitimate operations of non-profit organizations and on exclusively humanitarian activities.[31.]

[28] FATF, Partnering in the Fight Against Financial Crime: Data Protection, Technology and Private Sector Information Sharing, (Paris, 2022), p. 64, available at www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf.coredownload.pdf.

[29] High-Level Synopsis of the Stocktake of the Unintended Consequences of the FATF Standards, 27 October 2021.

[30] Benjamin Vogel, "Potentials and limits of public-private partnerships against money laundering and terrorism financing", 2022, available at https://eucrim.eu/articles/potentials-and-limits-of-public-private-partnerships-against-money-laundering-and-terrorism-financing/ .

[31] Global Counterterrorism Forum, Good practices memorandum for the implementation of CFT measures while safeguarding civic space, September 2021, available at www.thegctf.org/Portals/1/Documents/Links/Meetings/2021/19CC11MM/CFT%20GP%20Memo/CFT%20Memo_ENG.pdf?ver=fahs72ucLyyYOTj7WDwBkQ%3D%3D.

Another challenge that applies to Member States' broader CFT efforts is the effective institutionalization of gender considerations into CFT measures, including those produced by cooperation with the private sector. In this regard, insufficient efforts have been reported on how States consider gender implications within their PPP frameworks and establish mechanisms to monitor and evaluate outcomes. As States enter into more information-sharing arrangements with the private sector, it is essential to ensure that the typologies and preventive measures developed or tactical information shared within the framework of the PPP do not disproportionately affect any gender, including by limiting financial access.

As information-sharing between the private and public sectors progresses, competent authorities will need to increasingly consider the potential impact of preventive measures and accordingly adjust working arrangements and frameworks.

USE OF NEW OR DEVELOPING TECHNOLOGIES FOR INFORMATION-SHARING WITH THE PRIVATE SECTOR

As both public and private actors handle more complex data, technologies play an increasingly important role. PPPs often involve the use of technology such as communication platforms or data analytical tools in analysing and exchanging information. A number of States reported that they had developed communication platforms to allow for the sharing of information between the public and the private sectors. The use of new technologies in PPPs represents an important opportunity, as they can be built to process data securely, for a specific purpose, in a way that is more accurate and timelier, in particular when compared to States that rely on paper-based systems.[32]

At the same time, developing technologies that facilitate increased information-sharing between the private and public sectors requires responsible and innovative approaches focused on relevance and effectiveness, but which also incorporate appropriate mitigation measures. These measures should be in line with the principles of necessity, proportionality, legality, and non-discrimination under international human rights law, as well as the risk-based approach under the FATF Standards.[33] For example, privacy enhancing technologies can also help to address concerns related to data protection (e.g.,

[32] FATF, *Opportunities and Challenges of New Technologies for AML/CFT*, (Paris, 2021), available at www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf.coredownload.pdf.

[33] CTED's tech sessions: Highlights on "Threats and opportunities related to new payment technologies and fundraising methods", available at www.un.org/securitycouncil/ctc/news/cted%E2%80%99s-tech-sessions-highlights-%E2%80%9Cthreats-and-opportunities-related-new-payment-technologies-0.

when technologies allow for the analysis of encrypted data without exposing the identity of individuals).

In addition to the complexities and costs involved in developing or updating systems that seek to innovate AML/CFT frameworks, such as regulatory technology (regtech) and supervisory technology (suptech), operational challenges relating to different data formats, lack of interoperability between systems, or absence of secure communication platforms may hinder information-sharing efforts between stakeholders.

In light of this, the importance of data privacy and the ethical handling of data has become a critical challenge. For example, the Kingdom of the Netherlands' FIU recently shared its intention to integrate data privacy and ethical handling of data into the process of developing technology and partnerships. This work is currently under way.

Furthermore, CTED's consultations indicate that the existing PPP frameworks are at an early stage and do not sufficiently cater for the efficient exchange of information. It would be helpful to have regulations for the private sector to deliver data in electronic format and in standardized ways.

CONCLUSIONS

As States increasingly turn to the private sector to enhance AML/CFT frameworks and respond to the evolving tactics of terrorist financers, there is a crucial need for cooperation within a legal framework that defines the conditions under which competent authorities can access terrorism-financing-related data and expertise available in the private sector.

The evolution of financial methods also requires an engagement with a wider range of stakeholders, beyond traditional financial institutions. The fact that existing partnerships with the private sector are mainly with traditional financial actors poses challenges for States to comprehensively understand the latest threat.

Establishing robust and clear legal frameworks that comply with relevant human rights standards, in particular rights to data protection and privacy, to promote effective PPPs, is key to effectively exchanging information between the competent national authorities and private sector entities. More inclusive partnerships with a wider range of stakeholders have proven helpful to make PPPs work in the current landscape of the financial industry.

Well-established PPPs can serve as valuable models for successful partnerships for other Member States, with the lessons learned key to persuading competent authorities to allocate sufficient resources, time, and effort. In this regard, CTED will continue to monitor trends and developments on Member States' efforts to effectively cooperate with the private sector, acting in cooperation with all relevant partners and stakeholders (including FATF and its Global Network) with a view to identifying good practices and making recommendations for strengthening Member States' capacity in this area.