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

CTED Analytical Brief
December 2023

TABLE OF CONTENTS

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 better 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

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.

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 jogps n bujpo! i fme!cz!u i f!qvcmjd!t fdups-!u i f!qsjwbuf!t fdups!jt!pgu fo!#!efqsjwfe!!!pg!jogps n bujpo! 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-

scope and threats posed by terrorism financing for specific sectors, key patterns in

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

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 techy 0lving (n)-7(a)4nd

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, bt!qbsu!pg!Tubuf t!!BNM0DGU! 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 incidencesp targeted

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 ufsspsjt n !gjobodjoh!! 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

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 qsjwbuf!tfdups!t!tfbsdi!bmhpsjuint-!uif!ǳjoejsfduǈ!qspdfttjoh!pg!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] Hvjejoh!Qsjodjqmft!po!Cvtjoftt!boe!Ivnbo!Sjhiut-!Jnqmfnfoujoh!uif!Vojufe!Obujpot!‟!Qspufdu-!Sftqfdu!boe!Sfnfez!!!gsbnfxpsl-!3122-!bwbjmbcmf!bu: https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf

26 Benjamin Vogel, ǳPublic- qsjwbuf!qbsuofstijqt!jo!uif!gjhiu!bhbjotu!uif!gjobodjoh!pg!ufsspsjtnǈ, 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] Obef{ieb!Qvsupwb-!ǳCfuxffo!uif!HEQS!boe!uif!police directive: navigating through the maze of information sharing in publicpqsjwbuf!qbsuofstijqtǈ, 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

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

CONCLUSyoTF1 0.08 Tf1 0 0 1 9.98 8 Tm0.35 0.5 0.9 rg0.36 0 gN0 1 0.27 2.4 Tm0 g0 G