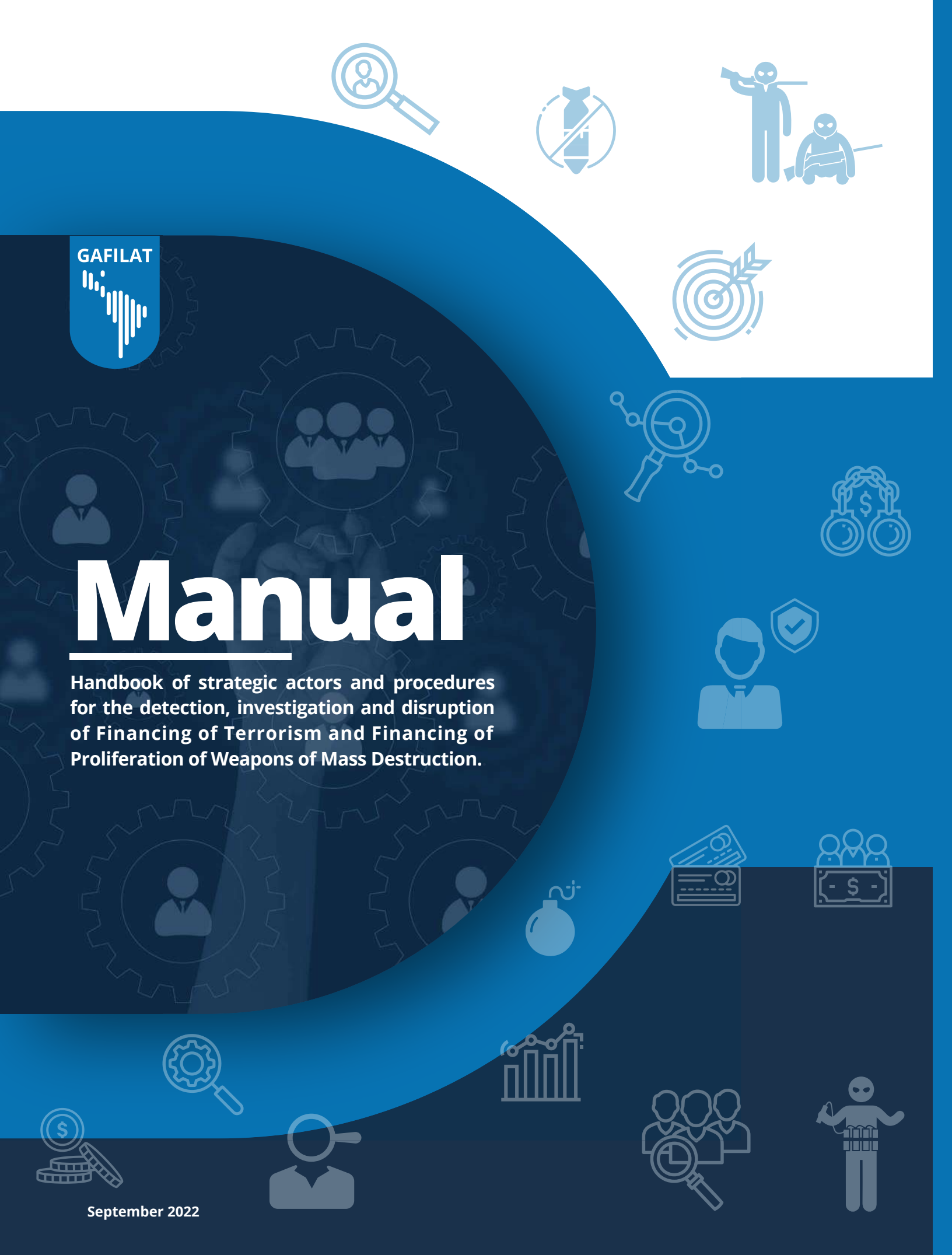
GAFILAT

Manual

Handbook of strategic actors and procedures for the detection, investigation and disruption of Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction.



September 2022

Handbook of strategic actors and procedures for the detection, investigation and disruption of Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction.

September 2022

Manual: Handbook of strategic actors and procedures for the detection, investigation and disruption of Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction.

Edition curated by: Financial Analysis Unit of the Dominican Republic (UAF-RD)

Cover art: Communications Division of the Financial Analysis Unit of the Dominican Republic (UAF-RD)

INDEX

LIST OF ABBREVIATIONS AND ACRONYMS

1	WMD	Weapons of Mass Destruction.
2	IAIS	International Association of Insurance Supervisors.
3	AML	Anti-Money Laundering.
4	MLA	Mutual Legal Assistance.
5	APG	Asia/Pacific Group on Money Laundering.
6	DNFBPs	Designated Non-Financial Activities and Professions.
7	PPP	Public-Private Partnerships.
8	AUSTRAC	Australian Centre for Transaction Reporting and Analysis.
9	CFP	Combating the Financing of Proliferation.
10	CFT	Combating the Financing of Terrorism.
11	UNSC	United Nations Security Council.
12	FTF	Foreign Terrorist Fighter.
13	NRA	National Risk Assessment.
14	PF	Proliferation Financing.
15	TF	Terrorist Financing.
16	FATF	Financial Action Task Force.
17	GAFILAT	Latin American Financial Action Task Force.
18	IACT	Inter-American Convention Against Terrorism or Convención Interamericana contra el Terrorismo (Spanish acronym).
19	FI	Financial Institutions.
20	INTERPOL	International Criminal Police Organization.
21	ISIL	Islamic State of Iraq and the Levant or Estado Islámico en Irak y el Levante in Spanish.
22	LEA	Law Enforcement Agency.
23	LOR	Letter Rogatory or Commission.
24	MOU	Memorandum of understanding.
25	OAS	Organization of American States.
26	IOSCO	International Organization of Securities Commissions.
27	WCO	World Customs Organization.
28	NPO	Non-Profit Organization.
29	RFAI	Ibero-American Network of Anti-Drug Prosecutors for its acronym in Spanish.
30	UNSCR	United Nations Security Council Resolution.
31	REFCO	Network of Prosecutors against Organized Crime for its acronym in Spanish.

32	**STR**	Suspicious Transaction Report.
33	**RRAG**	GAFILAT's Asset Recovery Network.
34	**TFS**	Targeted financial sanctions.
35	**ARS**	Alternative Remittance Systems.
36	**MVTS**	Money or Value Transfer Services or Money or Value Transfer Systems.
37	**TBML**	Trade Based Money Laundering or Trade Based Money Laundering in Spanish.
38	**TI**	Information Technology.
39	**TTU**	Trade Transparency Unit or Trade Transparency Unit in Spanish.
40	**FTZ**	Free Trade Zone.
41	**UNODC**	United Nations Office on Drugs and Crime.

EXECUTIVE OVERVIEW

1. While the threat of terrorism and the proliferation of weapons of mass destruction (**WMD**) in Latin America remains low overall, the countries of the hemisphere are aware of the risk posed by international terrorist groups and note with great concern the dangers inherent in exploiting the banking system, strategic trade regulations and informal economies of many states to finance terrorist activities and/or acquire **WMD** and their means of delivery for terrorist purposes. Current patterns indicate that the more complex and asymmetric the violence, the greater the risk of terrorists acquiring, developing, trafficking and/or using nuclear, chemical and biological weapons. An effective response to these threats requires a holistic approach from a multidimensional security perspective that includes international cooperation and information sharing as key pillars.

2. For most Latin American countries, the proper use of counter-terrorist financing and counter-proliferation financing of **WMD (CTF/CPF)** tools has proven to be a major challenge. While the region faces significant security threats, these are generally related to organized crime rather than terrorism or proliferation per se. In fact, during the period 2002-2019 the region, despite representing approximately 8.5 percent of the world's population, had only 1 percent of the world's deaths from terrorism, 3 percent of the world's attacks from terrorism, and 4 percent of global economic impact from terrorism. [1]

3. The risks faced by the countries of the hemisphere in combating the **financing of terrorism (FT)** and the **financing of proliferation (FP)** of **weapons of mass destruction (WMD)**, as well as the money laundering **(LA)** associated with these criminal activities, have a direct impact on the integrity of financial institutions and sectors, as well as on their national economies in the broadest sense, discouraging foreign investment and distorting international capital flows. Those who finance terrorism and proliferation with **WMD** weapons take advantage of the inherent complexity of the global financial system and the lack of uniform legislative and operational treatment in countries' national policies, and are particularly attracted to jurisdictions with inadequate or ineffective control systems to where it is easier to transfer their funds undetected, taking advantage of existing weaknesses in information exchange mechanisms under international cooperation and **mutual legal assistance (MLA).** The porosity of land borders, ports and free trade zones in the region presents an added vulnerability due to the increased risk inherent in the informal nature of some **TF/PF** channels (bulk cash smuggling, informal remittances), as well as the prevalence of trade-based money laundering channels **(TBML).**

4. As part of a comprehensive approach, and in accordance with the obligations arising from the 19 international instruments on the subject, States must establish adequate measures and effective legislation to freeze without delay funds linked to terrorist pur-

1. Yansura, J.; Mavrellis, C.; Kumar, L.; Helms, C. 2021. Financial crimes in Latin America and the Caribbean: Understanding country challenges and designing effective technical responses. Global Financial Integrity. Washington DC.

poses. Furthermore, in accordance with recommendations 5, 6 and 7 of the **Financial Action Task Force (FATF)** and in accordance with article 4 of the **Inter-American Convention against Terrorism (IACT),** countries must implement targeted financial sanctions regimes to comply with **United Nations Security Council Resolutions (UNSCR)** related to the prevention and suppression of terrorism[2] , the proliferation of WMD and their means of financing.[3]

5. Since the adoption of **UNSCR** 1373 (2001), Latin American countries have expressed their strong commitment to the global response to terrorism and have made significant progress in fulfilling their obligations under international law by strengthening their criminal justice systems and operational capacities to detect, investigate, interdict and prosecute **terrorist financing (TF)** and **proliferation financing (PF)** networks of **WMD**. More than two-thirds of the states in the region have recently adopted legislation in accordance with the 19 relevant international counterterrorism instruments and **UNSCRs** and have improved their areas of international cooperation and interagency coordination, particularly within the framework of the Financial Action Task Force for Latin America **(GAFILAT).** However, the process of implementation of international instruments and **UNSCRs** to prevent and combat terrorism, **WMD** proliferation and their financing is uneven among **GAFILAT** member states. In addition, there are different levels of ratification and implementation among these countries of the universal and regional legal instruments against terrorism and its financing. To date, 25 countries in the hemisphere have ratified the **IACT.**

6. While other **UNSCRs** (such as 1267/99, 1373/01, 1988 and 1989 of 2011; among others) already addressed the aspect of combating the financing of terrorism in some form, Resolution 2462 (2019) is the first resolution that the Security Council has dedicated to the prevention and suppression of terrorist financing in a particular way. The resolution brings a new focus on terrorist financing risks and urges all states to assess their respective risks. It also highlights the value of financial intelligence in the fight against terrorism, including the detection of terrorist networks and their financiers. In it, the Council calls upon Member States to consider establishing, in accordance with international law, appropriate laws and mechanisms to allow for the widest possible international cooperation, such as the appointment of liaison officers, cooperation between law enforcement agencies, prosecutors' offices, judicial authorities and/or police forces, the creation or use of joint investigative mechanisms and better coordination of cross-border investigations in cases involving terrorism, its financing and organized crime, whether domestic or transnational. In general, it can be concluded that, although the countries of the region adhere to international standards on **CTF/CPF,** the absence of real threats linked to terrorism and/or **WMD** proliferation means that most of them do not have the necessary capabilities to use these tools and lack strategic procedures for their proper implementation. However, the absence of concrete threats in the region does not prevent countries from adopting strategic decisions and developing both preventive and repressive capabilities against **FT/FP.**

7. Based on the typologies of **ML** and **FT/PF** in the region, it can be stated that, although in recent years Latin American states have made significant progress in implementing the **FATF Recommendations and the UNSCRs** thanks to the range of legal reforms carried out and improved partnerships at the international, regional and sub-regional levels, the countries of the hemisphere still face significant challenges that prevent them from achieving a satisfactory level of effectiveness in preventing, detecting and combating **FT/PF.** Among the existing weaknesses are the absence of national **CTF/CPF** strategies and risk assessment methodologies; insufficient specialization of law enforcement agencies **(LEAs)** to investigate and prosecute **TF/PF** cases; limited use of special investigative techniques, **mutual legal assistance (MLA)** and joint investigation teams and lack of experience of **financial intelligence units (FIUs)** in the matter. In addition, the weakness of the Customs supervisory regime over trade and financial transactions, especially in free trade zones **(FTZs),** together with the lack of communication and information sharing between LEAs, FIUs and Customs are additional factors of concern with respect to FP-related WMD activities.

8. The capacity of **FIUs** in the region, including those that are members of the **Egmont Group**, must be strengthened, since most Latin American states have insufficient capacity to freeze funds and assets linked to terrorism and **WMD** proliferation. On the other hand, it is necessary to make legal amendments to the Codes of Criminal Procedure and administrative sanctioning laws of the countries of the hemisphere to implement a comprehensive system of investigation and punishment of **TF** and **PF** to remedy the lack of specialization in the matter of the **LEAs** and **FIUs.** Additionally, the strengthening of the regulations and processes in the area of forfeiture of ownership for jurisdictions that have these figures in their internal regulations and the implementation for those jurisdictions that do not have them should be encouraged. The absence of special procedures for the prosecution of **TF** crimes and the lack of criminal liability of legal persons in many legislations have been identified as two of the main challenges to prosecute these criminal conducts.

9. All these circumstances, together with the emergence of the Islamic State in 2014 as a new global terrorist threat, its subsequent defeat in 2019 and the takeover of Afghanistan by the Taliban regime in 2021, along with the risks arising from the return of foreign terrorist fighters to their countries of origin or to third States and the use of organized crime routes ("cocaine route") as alternative transit routes to access the hemisphere, highlight the need to strengthen the legal and procedural frameworks of the countries of the region so that

2. UNSC Resolutions 1267 (1999); 1373 (2001); 1988 (2011); 1989 (2011); 2178 (2014); 2253 (2015); 2322 (2016); 2368 (2017); 2396 (2017); 2462 (2019) and 2482 (2019).

3. Security Council resolutions implementing targeted financial sanctions related to WMD proliferation financing are 1718 (2006), 1874 (2009), 2087 (2013), 2094 (2013), 2270 (2016), 2321 (2016), and 2356 (2017). Resolution 2231 (2015), which endorsed the Joint Comprehensive Plan of Action (JCPOA), terminated all provisions of resolutions related to Iran and proliferation financing, including 1737 (2006), 1747 (2007), 1803 (2008), and 1929 (2010), but established restrictions including targeted financial sanctions. This lifting of sanctions is part of a step-by-step approach with reciprocal commitments endorsed by the Security Council. The JCPOA implementation day was January 16, 2016. Resolution 1540 (2004) and successive, prohibits WMD proliferation and its financing, but does not impose targeted financial sanctions.

they can face these new challenges and provide the relevant actors with strategic procedures for the detection, investigation and disruption of **FT** in the region, These developments highlight the need to strengthen the legal and procedural frameworks of the countries of the region to enable them to meet these new challenges and to equip the relevant actors with strategic procedures for detecting, investigating and disrupting **FT/PF.**

10. The handbook aims to strengthen the technical capacities of prosecutors, judges, police officers, customs agents and financial intelligence analysts in the region and to improve inter-institutional coordination mechanisms and international, regional and sub-regional cooperation among **GAFILAT** member states to detect, investigate and punish **TF/PF**-related activities in accordance with the **UNSCRs** and the 19 international instruments on the subject.

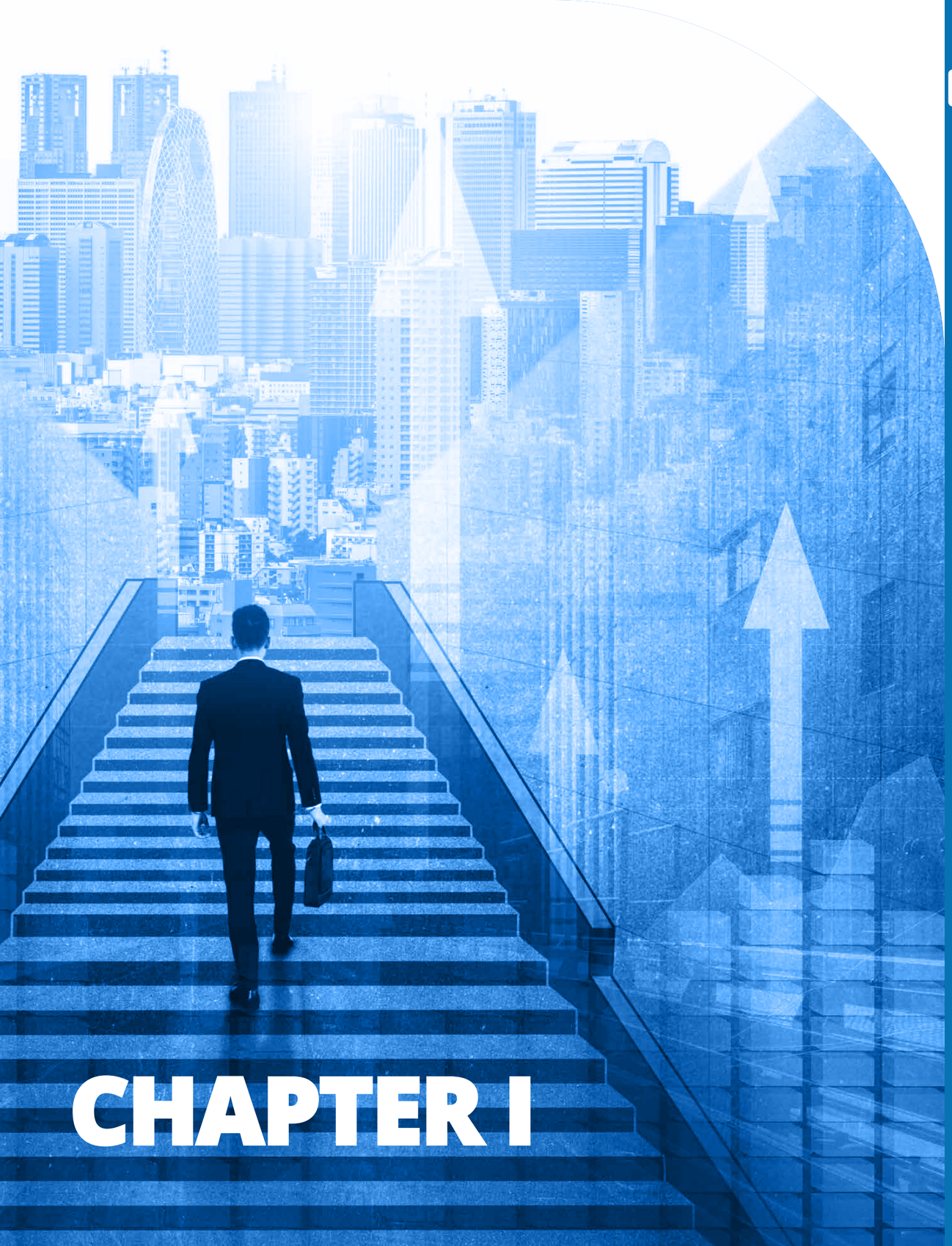
11. The handbook is divided into three chapters that address three core aspects of detecting, investigating and disrupting **TF/PF.** The first chapter focuses on the identification of strategic national actors in the fight against **FT/FP** with special attention to the cooperation mechanisms between **FIUs, LEAs and Customs**, the requirements for access to information, the particularities of cross-border currency transportation, trade-based money laundering **(TBML), alternative remittance systems (ARS)** and free trade zones **(FTZ),** as well as the existing international good practices in the framework of national **CTF/CPF** coordination mechanisms. The need for good inter-agency coordination between the authorities involved in the prevention, detection, investigation and disruption of **TF/PF** implies the need to share a harmonized approach in the adoption of risk analysis and the implementation of preventive and repressive measures that allow a rapid and fluid exchange of information in real time between the various agencies through a combination of formal (through a dedicated coordinating body) and informal communications, which can play a crucial role in analysis and investigation to build the necessary trust between the relevant actors. Coordinated action by financial intelligence experts is critical for the regime to be effective. This includes **FIU staff,** criminal investigators, prosecutors, judges, regulators, customs officials and employees of financial institutions. States have understood that the central intelligence agency does not function without the direct support of entities such as **FIUs**, the judiciary and the prosecutor's office, as well as other administrative entities such as customs or tax services. Under this scheme, national legislations have been modified to facilitate a fluid exchange of information between the different entities with competence in the matter.

12. The second chapter is devoted to strategic procedures for detecting, investigating and disrupting **TF/PF** through a detailed analysis of **TF/PF** indicators, the particularities and best practices in analyzing and investigating **TF/PF** cases, and the advantages of using parallel financial investigations and teamwork. In practical terms, counter-terrorism, **WMD** proliferation and **TF/PF** investigations are generally linked, although it is important to note that they need not be. To ensure that all relevant actors in the criminal network are uncovered, it is important to conduct systematic parallel financial investigations on a case-by-case basis, either through a stand-alone **FT/FP** investigation, or where appropriate, as part of a broader terrorism or **WMD** proliferation offense investigation. Many jurisdictions face challenges in being able to conduct parallel financial investigations, as financial investigations are generally not conducted if the underlying terrorist activity appears to be primarily self-funded or if the sums involved are very small. Good practices include ensuring that a **TF/PF** investigation can be initiated without an underlying terrorism or **WMD** proliferation case, and that the **TF/PF** investigation can continue even when the linked terrorism or **WMD** proliferation investigation has already concluded. Another useful practice is to issue manuals and procedures for identifying and investigating F**T/FP.** In addition, financial investigations should be considered not only from a prosecution-oriented perspective, but also from an intelligence standpoint.

13. The third chapter addresses strategic procedures in the framework of international cooperation, with particular reference to **joint transnational investigation teams (JITs), mutual legal assistance (MLA)** and other informal information-sharing mechanisms, as well as existing good practices in the field to improve the effectiveness of transnational investigations. International standards have recognized the value of forming **JITs** for the purposes of cross-border investigations where an offense involves multiple jurisdictions. The Interpretative Note to **FATF Recommendation 40** on International Cooperation suggests that **LEAs** should be able to form **JITs** to conduct cooperative activities in the course of their **TF/PF** investigations. Traditionally, **JITs** were formed only in offenses related to transnational organized crime and the financial aspect of an investigation was often forgotten or not included in **JIT** arrangements. However, current trends in many countries seek to ensure that financial investigation linked to **FT/FP** is included in any **JIT** agreement. **GAFILAT** jurisdictions would benefit from joining this emerging practice.

14. Three annexes complete the handbook. The first annex lists investigations and convictions in **TF/PF** cases in **GAFILAT** member states. The second annex includes a model agreement for the creation of a transnational **joint investigation team (JIT).** The third annex is dedicated to a case study on cooperation between **LEA-FIU** in a **FT** scheme through e-wallets.

15. The best practices and international experiences contained in the handbook will contribute to strengthening the regulatory and operational **CTF/CPF** frameworks of **GAFILAT** member states to effectively address these threats. Through this initiative, countries will be better able to address new mechanisms and sources of financing for terrorist activities; the transnational flow of illicit and licit money used to commit terrorist and **WMD** proliferation offenses; the movement of terrorists and their financial assets; and the illicit use of legal persons for such purposes, among others. Finally, it is expected to result in increased international cooperation, more effective information exchange and strengthened mutual legal assistance **(MLA)** among the countries of the region in the analysis, investigation, prosecution and punishment of terrorist and **WMD** proliferation offenses and their means of financing.



CHAPTER I

NATIONAL STRATEGIC ACTORS IN THE DETECTION, INVESTIGATION AND DISRUPTION OF TF/PF.

1. INTRODUCTION

16. Inter-institutional coordination is one of the greatest challenges in the implementation of national frameworks for combating **CTC/CFP of WMD**. From the very conception that the fight against **CTF/CPF**, in the international sphere, should be a multilateral effort, and in the domestic sphere an undertaking of all the actors involved in the institutional, social and economic life of a country, it is clear that cooperation and coordination in the prevention, repression and punishment of the phenomenon of terrorism and the proliferation of **WMD** and their means of financing does not belong to the control of a single national entity and that, on the contrary, responsibility should be distributed according to the capabilities of each agency with competence in the matter. Interagency coordination at the national and international levels works best when all relevant entities are involved and operate with a shared understanding of existing **TF/PF** typologies that allows them to adopt a common agenda that facilitates the greatest possible exchange of information and the best possible interagency cooperation.

17. A fully effective global effort to combat **TF/PF** benefits from well-functioning, transparent and corruption-free economies equipped with appropriate legal and regulatory frameworks and effective institutional capabilities to enforce laws and collect, analyze and share real-time intelligence and documentary evidence within and across national borders. Coordinated action by financial intelligence experts is critical for the regime to be effective. This includes **FIU** staff, criminal investigators, prosecutors, judges, regulators, customs officials and employees of financial institutions. States have understood that the central intelligence agency does not function without the direct support of entities such as the **FIU**, the judiciary and the prosecutor's office, as well as other administrative entities such as customs or tax services. Under this scheme, the domestic legislation of the countries has also been modified to facilitate a fluid exchange of information between the different entities with competence in the matter.

18. There is certainly a need for good coordination and communication between the various authorities involved in the prevention, detection, investigation and disruption of **TF/PF**. This implies the need to share a harmonized approach in the adoption of risk analysis and the implementation of preventive and repressive measures that allow for a rapid and fluid ex-

change of information between agencies through a combination of formal (through a dedicated coordinating body) and informal communications, which can play a crucial role in building trust between the relevant actors.

19. However, developing these institutional capacities is difficult and costly, and requires sustained political commitment. The complexity arises from the problems associated with achieving and maintaining cooperation among various public and private actors. Many countries have encountered difficulties in establishing legal, administrative and institutional arrangements for a variety of reasons, including legal restrictions and budgetary constraints. International cooperation initiatives, such as the training of new personnel in one country by experienced personnel in another, can make a valuable contribution to improving the capacity of relevant national agencies and strengthening the **PIC/PTC** prevention and control regime.

2. STRATEGIC AGENCIES AND AUTHORITIES IN THE CTF/CPF FRAMEWORK

20. The implementation of the **UNSCRs** and the **targeted financial sanctions (TFS)** regime in the **CTF/CPF** framework involves a variety of agencies at both the policy and operational levels, and some of these agencies may not be involved in the **anti-money laundering (AML)** framework.

21. The following is a list of the agencies or authorities commonly involved in the implementation of the **UNSCRs** on **TF/PF**, including enforcement, compliance monitoring and information exchange, although this may vary from country to country:

- ***Policy departments:*** *introduce changes to the domestic or jurisdictional regime and identify gaps in the regime. Examples include foreign affairs, finance, trade, commerce, interior and justice departments;*

- ***Financial and non-financial supervisors, competent authorities and SRB:*** *conduct regulation, supervision and enforcement to ensure that access to **FT/FP** is denied;*

- ***Export control, customs and border agencies:*** *ensuring compliance with export controls, stopping shipments from sanctioned suppliers or to a designated end user (or by suppliers or end users of interest), exchanging financial information or relevant customer data that could be useful to detect actual end users and illegal transactions and could facilitate **LEA** investigations by enabling a deeper understanding of the transaction, business structures and methods used to facilitate illegal transfers of prohibited items in all jurisdictions. As users of information, export control authorities have noted that financial information can be useful for export control authorities to be able to detect actual end users and illegal transactions and enhance the effectiveness of investigations conducted by law enforcement authorities by enabling a deeper understanding of the transaction and business structures and methods used to facilitate illegal transfers of prohibited items in all jurisdictions. Therefore, export control and customs agencies are both providers and recipients of information in the context of the **CTF/CPF** fight;*

- ***Intelligence services:*** *identify, analyze and disseminate intelligence on persons or entities that may be involved in or supporting **TF/PF** activities;*

- ***Financial intelligence units:*** *to receive, analyze, process, evaluate and transmit information for the detection of **ML** and/or **FT/FP**, as well as to assist in the implementation by regulated entities of the prevention system to detect suspicious transactions of **ML** and/or **FT/FP**. Although the **FATF** does not require suspicious transaction reports **(STRs)** on **PF**, some jurisdictions have chosen to establish reporting requirements for supervised institutions as an additional means to implement the **UNSCRs** on the matter. In addition, even in jurisdictions without **STR** requirements for **PF, FIUs** may receive **STRs** on **PF-related** activities that reporting entities have identified as a different type of illicit activity and may share this information with other competent authorities;*

- ***Law enforcement agencies:*** *investigate and prosecute **FT/FP**-related offenses and apply criminal, administrative and/or civil penalties for violations of laws and regulations;*

- ***Trade and investment promotion agencies:*** *identify and analyze **TF/PF** risks associated with sanctioned countries when considering, and prior to facilitating trade; and*

- **Other agencies or authorities:** *responsible for implementing the requirements of the **UNSCR**.*

22. In particular, the following key agencies are usually involved at the operational level:

- *Ministry of Justice*
- *Public Prosecutor's Office*
- *Ministry of the Interior / investigation agencies / police*
- *Ministry of Finance / fiscal and tax agencies*
- *Financial Intelligence Unit **(FIU)***
- *Central Bank and other financial sector supervisors/regulators*
- *Supervisory authorities for FIs and designated non-financial businesses and professions **(DNFBPs)***
- *Customs authorities*
- *Anti-corruption authorities*

23. The incorporation of all the agencies identified above to coordinate the implementation of the **UNSCRs** is a critical way to combat **TF/PF**, and allows for joint analysis, coordinated and complementary operations, and the implementation of more developed policy positions. Such coordination and cooperation can also be a key measure of trust and interagency relationship building. One possible avenue for achieving this cooperation, information exchange and joint coordination may be regular or ad hoc meetings that may include representatives of the above-mentioned agencies. Issues that can be discussed at these meetings include:

- *Monitoring and analysis of risks, threats, new trends and vulnerabilities in **FT/FP;***
- *Development of policies to combat **FT/FP;***
- *Recommendations for appropriate responses for competent agencies to take action to counteract **TF/PF;***
- *Identification of key intelligence gaps related to **TF/PF** and the development of possible solutions to close those gaps;*
- *Consideration of possible interdiction opportunities to prevent **TF/PF** and coordination of such actions;*
- *Coordination of the activities of competent agencies (including competent financial and non-financial regulatory and supervisory, intelligence and law enforcement authorities) in terms of combating **TF/PF;***
- *Coordination of financial support investigations for export control violations and enforcement of laws related to the export and transshipment of controlled dual-use items, including sanctioned countries;*
- *Coordination of potential plans by financial and non-financial regulators and supervisors, intelligence and law enforcement to identify and designate persons and entities that may be involved in or supporting **TF/PF;** and*
- *Review of mechanisms to ensure effective scrutiny of suspicious activity reports and to comply with sanction implementation requirements.*

24. The **FATF** recommendations require countries to establish the necessary legal authority and identify the competent agencies responsible for implementing and enforcing the **TFS** and to have in place cooperation and, where appropriate, coordination mechanisms to combat **TF/PF.** Specifically, **FATF Recommendation 2** emphasizes the need for greater interagency cooperation and advises countries to institute a coordination mechanism to review the **AML** and **CTF/CPF** regimes. The scope of the **Recommendation** goes well beyond the issue of internal coordination, as it aims to measure the effectiveness of the **AML** and **CTF/CPF** regimes. However, such a measure cannot be undertaken outside of an interagency process and undertaking such an assessment of effectiveness should be used as an incentive for national coordination and information sharing. While the **FATF** standards do not impose a specific supervision or monitoring model, being able to identify relevant bodies and link them in the **TF/PF context could support the implementation of Immediate Outcomes 10 and 11 and Recommendations 6 and 7, as well as Recommendation 2.**

25. Based on a review of the findings of the mutual evaluations on the level of technical compliance and the effectiveness of countries in implementing **TFS,** the lack of inter-agency cooperation and coordination is a common weakness identified in the **TF** context and even more so in the **PF** area.

26. Among the main deficiencies identified are the following:

- *Lack of legal and institutional frameworks to implement the institutional cooperation and coordination mechanisms required by the **FATF** in the **TF/PF** framework;*
- *Lack of identification of key agencies in the **CTF/CPF** fight;*
- *Failure to establish a committee to coordinate or be in charge of supervision, enforcement or disclosure related to **FT/FP;***
- *Lack of specific provisions in the law to expand the power of the main committee to coordinate and cooperate with other competent authorities on **TF/PF** related policies and activities;*
- *The coordinating committee involves only the authorities responsible for TF-related activities and not all authorities responsible for implementing the **PF-related** asset freeze participate directly in the committee, or are invited to participate even on an "as needed" basis.*

2.1. COOPERATION MECHANISMS BETWEEN UIF AND LEA

27. International and regional standards require countries to establish effective mechanisms for cooperation between competent national authorities, but do not provide or refer to any particular mechanism. With very few exceptions worldwide, **FIUs** are not responsible for conducting criminal investigations. Therefore, it is essential that strong legal remedies are in place to enable an **FIU** to provide information to LEAs with jurisdiction to investigate and prosecute **TF/PF** offenses identified by the **FIU** through its financial intelligence analysis activities.

28. In terms of international standards related to financial investigations, **FATF Recommendation 30** and the related Interpretative Note require that law enforcement agencies and other competent authorities be considered when countries make use of multi-disciplinary teams in financial investigations. However, among competent authorities, the Interpretative Note includes authorities that are not law enforcement agencies per se, but have responsibility for pursuing financial investigations of predicate offenses (e.g.

anti-corruption authorities), to the extent that these authorities are exercising functions covered under **Recommendation 30.**

29. Financial investigations should be applied at all stages of criminal investigations and prosecutions: from proactive identification of crime or criminal networks, through case investigation and evidence gathering, to prosecution and conviction of offenders. **FIU** information is one of the most frequent triggers for a financial investigation.

2.1.1. ACCESS BY THE UIF TO INFORMATION MANAGED BY THE LEA

30. While **FIUs** play an active role in financial investigations conducted by the various investigative agencies of the law enforcement branch, such as police forces for example, their participation in financial investigations is mandatory in only a minority of jurisdictions, while in most jurisdictions it is optional or depends on whether certain criteria are met. Legal restrictions and limitations concerning the protection of sensitive data and technical reasons related to **information technology (IT)** and the absence of integrated databases sometimes prevent **FIUs** from having direct access to relevant information managed by **LEAs**. The most common type of information that **FIUs** can access relates to criminal investigations, prosecutions, convictions and criminal records, with less access to information related to ongoing police operations and **MLA** processes.

31. The most common conditions for allowing direct **FIU** access to information managed by **LEAs** include:

- *Information provided to foreign **FIUs** should be used for intelligence purposes only.*
- *Permission is required before a foreign **FIU** can further disseminate the information.*
- *Certain conditions imposed by few **FIUs** are very restrictive, such as the need for a request for **mutual legal assistance (MLA)** or a **memorandum of understanding (MOU)** or the existence of legal prohibitions on the exchange of information.*

32. Based on the above considerations, the following criteria for **FIU** involvement in financial investigations in **TF/PF** cases could be considered good practices:

- *Where the financial investigation is based on information or reports from the **FIU**, it would make sense for the **FIU** to continue to work with the relevant **LEA** and actively participate in the financial investigation if it can contribute to the success of the case. If the **FIU's** involvement is active throughout the investigation of the case, care should be taken to safeguard the integrity and security of the investigation.*
- *The inclusion of **FIUs** in financial investigations conducted by **LEAs** should not be mandatory. The final decision on whether the **FIU** will participate in such financial investigation should be left to the **FIU**.*

2.1.2. LEA ACCESS TO INFORMATION MANAGED BY THE IFUIF

33. It is standard practice for the **FIU** to disseminate information and the results of its analysis to multiple **LEAs** simultaneously. Mechanisms to ensure that recipients coordinate their activity and make appropriate use of the information provided by the **FIU** include:

- *The Public Prosecutor's Office coordinates and takes the lead in a criminal investigation and, therefore, coordinates the activities of all **LEAs.***
- *A list of recipients is included in the **FIU** file and then it is up to the recipients to resolve any overlapping interests.*
- *An intergovernmental committee / body / working group coordinates any overlapping issues.*
- *Points of contact / focal points are assigned by the **FIU** and **LEAs** to coordinate with each other.*
- *Solutions are provided in the Code of Criminal Procedure, other legal norms or in an **MOU**.*
- *The **FIU** will act as a coordinator and organize meetings with all relevant stakeholders as necessary.*
- *There are feedback mechanisms from the **LEAs** to the **FIU** on how the information will be used.*

34. Information contained in reports disseminated by the **FIU** to **LEAs** should be treated as confidential. The protection of **FIU** information is regulated by the general security regulations, the **AML** and **CTF/CPF** legislation, the Codes of Criminal Procedure, and the **MOUs** or interdepartmental agreements signed between **FIUs** and **LEAs.** To ensure compliance with secrecy rules, documents provided by **FIUs** are stamped and marked as classified, and include disclaimers and/or caveats. In the same vein, **FIUs** use secure channels for dissemination, such as secure online systems **(such as a GoAML message board)**, secure telephone/fax, or through a **"secret department"** that records all letters, including senders and recipients. National legislation also stipulates penalties for breach of confidentiality rules.

35. Conditions that allow for the withdrawal of confidentiality include:

- *The recipient is empowered to decide whether it is appropriate to remove or reclassify information, without specifying the conditions.*
- *The President of the Government has the authority to withdraw confidential status in any particular case when this does not affect the safety of the sources, the State, or any of the officials involved in the case.*
- *The procedures for the withdrawal of confidentiality are prescribed by law for the protection of confidential information.*
- *Specific authorization/consent from the FIU based on a written and well-explained request provided by the recipient.*

36. Specific authorization/consent from the **FIU** based on a written and well-explained request provided by the recipient:

DIRECT ACCESS TO INFORMATION	OBLIGATION TO SHARE INFORMATION SPONTANEOUSLY	ABILITY TO SHARE INFORMATION SPONTANEOUSLY
Australia	Germany	Austria
United States	Belgium	Canada
Ireland	Chile	Denmark
Netherlands	Korea	Finland
United Kingdom	Spain	Greece
	Slovenia	Japan
	France	Luxembourg
	India	Norway
	Iceland	New Zealand
	Italy	
	Mexico	
	Portugal	
	Czech Republic	
	Slovak Republic	
	South Africa	
	Sweden	
	Switzerland	
	Turkey	

37. The following mechanisms are used in several jurisdictions to strengthen cooperation between the **FIU** and the competent **LEAs:**

- *LEA and/or FIU personnel acting as liaison officers.*
- *Designation of contact points in the relevant **FIUs** and **LEAs** to address operational and other bilateral issues of common interest.*
- *Regular meetings and formal and informal daily and direct contacts to provide a forum for the exchange of case-related information, obtain feedback, discuss practical problems and obstacles, and promote training activities.*
- *Signing of bilateral or multilateral **MOUs** between the **FIU** and competent **LEAs. MOUs** are mainly used in jurisdictions where **FIUs** are not attached to **LEAs.** They are generally aimed at improving information exchange. Often, such **MOUs** also seek to establish mechanisms to enhance cooperation and coordination of activities between the parties.*
- *Establish joint working groups to address operational/case-based issues **(such as analysis and/or investigation of complex LA, TF/PF cases)** or other, strategic issues **(such as national risk assessment of LA and TF/PF, developing IT solutions for information sharing, etc.).***
- *Conducting joint training, including the exchange of personnel for training purposes and promotion of internship programs.*
- *Conducting internal surveys to understand the needs of **FIUs** and how to improve cooperation with **FIUs.***

38. From an operational point of view, the use of liaison officers attached to either the **FIU** or the **LEA** or both is considered one of the most effective cooperation mechanisms. The following common practices with respect to the role of **LEA** liaison officers in **FIUs** should be noted:

- *Most often, **FIUs** use liaison officers to share intelligence information with **LEAs**, or to obtain information from **LEAs** that is needed to perform **FIU** tasks.*
- *Some **FIUs** use liaison officers as analysts who are in charge of conducting financial analysis of **SARs** or other information received.*
- *In other cases, liaison officers are also used to coordinate investigative teams when **FIU** reports are connected to an ongoing **LEA** investigation or when detailed and customized **FIU** intelligence reports are needed.*
- *In some **FIUs**, liaison officers are used to coordinate meetings, organize workshops and advise FIUs on investigative techniques and other law enforcement matters.*

39. The performance of the following tasks by **FIU** liaison officers in **LEAs** is considered good practice:

- *Follow-up of cases reported by **FIU** to **LEAs.***
- *Support **LEAs** through operational financial analysis of cases under investigation.*
- *Coordinate actions during joint investigations.*
- *Act as facilitators during the exchange of information.*
- *Facilitate cooperation related to strategic analysis.*
- *Support **LEAs** in providing feedback to **FIUs.***
- *Train **LEAs** in the use of financial intelligence tools.*

40. In most cases, the role and legal status of liaison officers is regulated in the **MOU** or similar agreement signed by the **FIU** and the competent **LEAs.** Only a few jurisdictions include it in their legislation. The following table lists the existing advantages and obstacles to cooperation between **LEAs** and **FIUs.**

ADVANTAGES OF COOPERATION BETWEEN LEA AND UIF.	OBSTACLES TO COOPERATION BETWEEN LEA AND UIF.
Legal clarity on the rights and obligations of both parties.	Legal barriers: Information sharing legislation is too restrictive; **FIU** can only support **LEA** investigations of **ML** and/or **TF/PF**.
Well-developed cooperation procedures.	**LEA** requests sent to **FIUs** are intended to circumvent the procedures provided for in the Code of Criminal Procedure.
Understanding of each person's capabilities, priorities and needs.	There are misunderstandings about the role of the **UIF**.
Strong and well-developed relationship (direct personal contacts).	**LEAs'** knowledge of **AML/CFT/CPF** is inadequate.
Regular meetings and coordination (points of contact and need for experienced staff for coordination on both sides).	**LEAs** lack human and/or technical capacity to investigate financial crime.
Clear communication mechanisms.	**FT/FP** is not the **LEA's** priority.
Mutual trust and commitment.	**LEAs** submit incomplete applications.
Timely exchange of information without hindrance, including direct access to data, where permitted.	**LEAs'** responses are not timely.
Provision of detailed and useful information.	The **LEA** databases are not centralized.
Share experiences and knowledge on **LA and/or FT/FP** typologies and trends.	The **FIU** lacks direct access to some or all **LEA** databases.
Joint teams and/or joint investigations.	The information disseminated is not understood as expected and is not recorded in the **LEA** database in a timely manner.
Complete and timely comments provided by both parties.	
Creation of a review group to guarantee the quality of information exchange.	
Coordination with the Public Prosecutor's Office.	

2.2. COOPERATION MECHANISMS BETWEEN THE IFU AND CUSTOMS

41. The value added to the global economy, which represents faster and more efficient strategic trade and financial transactions, is accompanied by an increased challenge for Customs, **FIUs** and **LEAs** due to the potential exploitation by transnational organized crimeand terrorist organizations that regularly smuggle dual-use goods for **WMD** proliferation purposes and launder their assets across international borders. Customs and **FIUs** traditionally represent two of the four main law enforcement pillars for combating **LA**, financial crime, smuggling and **FT/FP** activities. The other two pillars are **LEAs** and tax authorities.

42. Customs, as the first line of defense at external borders and inland ports of entry, has a crucial mandate to identify and prevent the smuggling movement of currency/currency equivalents, precious gems/metals and other items of monetary value. Customs services face numerous challenges in detecting and controlling the cross-border transportation of currency and smuggling of dual-use goods related to **WMD** proliferation or for terrorist purposes, as they have jurisdiction over multiple ports of entry within their respective countries.

43. It is critical that the Customs service has an effective and efficient working relationship with other relevant agencies, especially **FIUs** and **LEAs,** when intercepting, seizing and investigating illicit currency trafficking and smuggling of dual-use goods across borders. The increasing complexities surrounding new **FT/FP** typologies require national customs services and **FIUs** to work together in a coordinated manner to counter this threat to national security and the stability of the financial system. In order to establish smooth cooperation between these agencies, it is important to ensure alignment of their internal policies to deploy their personnel and resources in the most effective manner. These challenges call for a coordinated and harmonized approach to **TF/PF** risk management and intelligence analysis, including financial intelligence.

44. **FIUs** have the responsibility to analyze suspicious financial transactions within their jurisdiction, including through declarations or disclosures of physical movement of currency and currency equivalents. Customs has an essential role in providing **FIUs** with relevant information on illegal and suspicious cross-border movement of currency and currency equivalents, as it is the only entity capable of providing such data to **FIUs**. By receiving such information, **FIUs** have the opportunity to link suspicious activity with other suspicious financial transactions identified by the financial industry and other public and private sources (**SARs,** police reports, etc.).

45. Export control agencies and customs services can benefit from the financial intelligence generated by the **FIU** and use the information provided on potential suppliers or end-users of dual-use items linked to **WMD** programs when deciding whether to grant an export license or authorize the passage of goods across their borders. Some jurisdictions have developed profiles of suspect suppliers based on the commission of violations of export control provisions or end-users based on the application by customs authorities of the catch-all clause.

46. The close relationship between **PF** safeguards and export control systems presents some risks that should be avoided. In particular, duplication of responsibilities from both the export control side (exporters or export control authorities); and the financial side (banks or competent authorities, including **FIUs**) could lead to loss or duplication of efforts. Taking into account the specificities of international financial flows and the characteristics of international trade finance, it is not possible to expect from **FIUs** the same type of controls that are mandatory for exporters prior to the export of dual-use items listed in international export control regimes.

47. The challenges in obtaining up-to-date and accurate information on the beneficial owner of legal structures is a vulnerability that impacts the degree of effectiveness of countries in terms of compliance and implementation of proliferation-related financial sanctions and their efforts to combat such criminal conduct. Challenges in identifying assets and funds of designated individuals and entities linked to the **PF** of **WMD** include the general use of legal structures by organized criminal networks to conceal their proliferation activities. Because individuals involved in proliferation activities frequently use front men to establish companies, including legitimate companies that carry out such activities and mix illicit and licit funds, it is extremely important for authorities to have access to reliable, truthful and up-to-date information to identify the ultimate beneficiary of these structures, especially in cases linked to the **DNFBP** sector.

48. Based on the above reasoning, it can be concluded that customs administrations play a key role in the prevention and detection of **TF/PF.** In addition to differences in the way the customs administration is structured as an agency, countries also adopt different models for determining the involvement of customs administrations in **TF/PF** investigations. The following table shows the countries where the customs administration is responsible for criminal investigations, those where the customs administration conducts investigations under the direction of a prosecutor, and those where investigations are conducted outside of the customs administration.

The customs administration directs and conducts the investigations.	The customs administration conducts investigations under the direction of a prosecutor.	A specialized tax agency, independent of the customs administration, conducts the investigations.	Investigations are conducted by the police or the Attorney General's Office.
Germany Australia Belgium Canada Korea United States Greece India Ireland Iceland Luxembourg New Zealand United Kingdom South Africa Switzerland	Austria Chile Spain Finland France Netherlands Portugal Czech Republic Slovak Republic Sweden Turkey	Italy	Denmark Slovenia Japan Mexico Norway

2.2.1. ILLICIT TRANSPORTATION OF FOREIGN EXCHANGE

49. The following are the areas where **TF/PF** cooperation between **FIU** and Customs is most relevant: i) Illicit transportation of currency; ii) Trade-based **ML (TBML)**; iii) Alternative remittance systems **(ARS)**; iv) Use of free trade zones **(FTAs)**; v) Use of the Customs and Border Protection Agency **(CBP)**; vi) Use of the Customs and Border Protection Agency **(CBP)**; vii) Use of the Customs and Border Protection Agency **(CBP)**; viii) Use of the Customs and Border Protection Agency **(CBP)**.

50. The most frequent modi operandi used for the illicit transportation of currency include:

- *Concealment by the passenger,*
- *Concealment inside cargo, vehicles, vessels and aircraft; and*
- *Concealment by mail.*

51. These modi operandi are typically used to smuggle foreign currency, currency equivalents (e.g., personal checks, official bank checks, money orders, traveler's checks, bearer bonds, etc.), as well as gems and precious metals.

52. Key practical recommendations for Customs and its officers to address these criminal activities include:

- *Provide training regime for Customs officers to include **LA** and **FT/FP** methods related to currency movement, concealment methods, intelligence based detection methods.*
- *Ensure that Customs arrival and departure areas have clear indications of the requirements for declaring or disclosing the transportation of minimum amounts of currency.*
- *Customs Services should also regularly consult the **FATF** International Best Practice Guide on Detecting and Preventing the Illicit Cross-Border Transportation of Cash and Bearer Negotiable Instruments and the **GAFILAT** Best Practice Guide on Monitoring the Cross-Border Transportation of Cash and Valuables.*[4]
- *Provide sound basic and advanced training on methods of smuggling vehicles, vessels, aircraft and conveyances, as well as methods of smuggling cargo and containers for Customs Service management and front-line officers.*
- *Conduct periodic field operations focused on transfers targeting the smuggling of currency and currency equivalents. These operations should include other **LEAs**, where possible.*
- *Provide **FIUs** with intelligence generated during customs control.*
- *Use intelligence derived from **FIU** analysis.*
- *Establish and maintain a close working relationship with national postal services and private express delivery companies.*
- *Trainings can be a useful tool to update knowledge, raise awareness and gather feedback from front-line officers in order to update typologies and indicator list.*

2.2.2. TRADE-BASED MONEY LAUNDERING (TBML)

53. Trade-based money laundering **(TBML)** is perhaps the most complex form of money laundering. **TBML** is an umbrella term for many different **LA** schemes and is recognized by the **FATF** [5]as one of the main methods of concealing the origin of illicit funds. The **FATF** defines **TBML** as the process of disguising the proceeds of crime and moving value through the use of commercial transactions in an attempt to legitimize their illicit origin. Identifying and tracking illicit currency are difficult tasks in themselves. When terrorist organizations convert illicit funds into commercial products, precious gems and metals, foodstuffs, or other marketable items and subsequently introduce them into global commerce, the investigator's task becomes increasingly difficult.

4. https://www.gafilat.org/index.php/en/biblioteca-virtual/gafilat/documentos-de-interes-17/buenas-practicas-18/1260-mejores-practicas-tte/file

5. https://www.fatf-gafi.org/media/fatf/content/Trade-Based-Money-Laundering-Trends-and-Developments.pdf

54. The challenge for analysts and investigators is to link fraudulent business activities to the predicate crimes that generate the illegal proceeds. The concerted efforts of **FIUs** and customs services are an invaluable tool in identifying and combating such intricate criminal activity. **FIUs** are the authorities responsible for receiving and analyzing suspicious transactions identified by the various financial and non-financial **SOs.** Meanwhile, customs services have the ability to identify suspicious/illicit activities linked to domestic and international trade.

55. Key recommendations for Customs and its officers to address these criminal activities include:

- *Through formal collaboration and information exchange between **FIUs** and customs services, **FIUs** are encouraged, in accordance with the respective national legal framework and in line with the general principle of independence and operational autonomy of **FIUs**, to provide financial intelligence to customs services linked to **TBML**.*
- *Customs is encouraged to conduct further analysis of this information in an effort to link **FIU** data with the **LA** and **FT/FP** phases.*
- *Due to the complexity of **TBML** schemes and the potential high volume of transactions involved, both **FIUs** and Customs are encouraged to establish training modules on **TBML** typologies in their training regimes. They are also encouraged to conduct cross-training programs.*
- *The creation of a specialized unit within Customs dedicated to addressing such **TBML** schemes, such as a cargo analysis team or a financial investigations unit, could be beneficial. The Trade Transparency Unit **(TTU)** is an example of a more advanced cargo analysis unit, whereby import and export data between independent customs services are shared cooperatively to promote a bilateral agreement. Consideration should also be given to the involvement of **FIUs** in such specialized units, or operational cooperation with **FIUs** if direct involvement is not possible.*
- *Conduct robust joint public outreach programs to the general public, finance companies, shipping companies, brokers, etc. regarding **TBML** and customs fraud schemes.*
- *Customs and **FIUs** are encouraged to participate and disseminate efforts with other **LEAs**, to include tax authorities, to increase awareness of such schemes among all relevant agencies.*

MEXICO

*Mexico's **Tax Administration Service (SAT)** has fostered interagency and international coordination for risk assessment and management of transnational organized crime and fraud threats by adopting **Trade Transparency Units (TTU)** for intelligence and information exchange between Mexico and the U.S. Mexico's tax and customs authority has adopted this tool to increase resilience to smuggling and establish links between tax evasion and national security threats. The use of **TTUs** to exchange information on the value of goods traded with the U.S. (Mexico's largest trading partner) allows for data validation and detection of illicit trade patterns and fraud. To do so, **TTUs** compare information on imports into Mexico with information on exports from the U.S. (and vice versa) in order to assess and develop risk frameworks to determine instances of non-compliance, misvaluation and potential fraud in trade. TTUs also facilitate the identification of routes, distribution points and sales of illicit goods. TTU's provide valuable information to **SAT** to conduct joint operations and investigations with the Attorney General's Office, the Navy, the Ministry of National Defense and the Federal Police.*

UNITED STATES

*The primary U.S. international effort to counter TBML is the **Trade Transparency Unit (TTU)** program under the **Department of Homeland Security's (DHS) Immigration and Customs Enforcement (ICE). ICE** established TTUs in 17 partner countries for the purpose of sharing and analyzing trade data to identify potential **TBML** cases. While TTUs have played a key role in some **LTBI** investigations, the TTU program has experienced several challenges, including lapses in information sharing between **ICE** and partner TTUs, different priorities between ICE and partner TTUs in conducting LTBI investigations, and limitations in the data system ICE and TTUs use. However, ICE has not developed a strategy to increase the effectiveness of the TTU program or a performance monitoring framework to evaluate the results of its work with partner TTUs. As a result, ICE does not have clear guidance on how best to operate the TTU program and cannot make management decisions based on program results.*

SPECIALIZED UNITS IN THE REGION

COUNTRY	YEAR OF CREATION	FREQUENCY OF INFORMATION EXCHANGE
Colombia	2005	Monthly
Argentina	2006	Weekly
Brazil	2006	Monthly
Paraguay	2007	Monthly
Mexico	2008	Monthly
Panama	2010	Monthly
Ecuador	2015	Monthly
Guatemala	2016	Monthly
Australia	2011	Monthly
Philippines	2012	Pending
Dominican Republic	2012	Monthly
Peru	2013	Monthly
France	2013	Biannual
Uruguay	2015	Quarterly
Chile	2017	Monthly
United Kingdom	2018	Annual
New Zealand	2019	Pending

2.2.3. ALTERNATIVE REMITTANCE SYSTEMS (ARS)

56. **Money or value transfer systems (MVTS)** refer to financial services that involve the acceptance of cash, checks, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the **MVTS** provider belongs. Transactions conducted by such services may involve one or more intermediaries and include a

final payment to a third party. Sometimes these services have links to particular geographic regions and are described using a variety of specific terms, including hawala, hundi and fei-chen; often referred to as alternative remittance systems **(ARS)** are transfer systems that exist exclusively or partially outside the regulated financial sector. **MVTS** include hawala systems, unregulated courier services and bureaux de change, as well as certain electronic currency transfer schemes, among other methods. **MVTS** may also include systems that involve the transfer of value through the conversion of proceeds to another method of holding value, from gems and precious metals to electronic storage devices, and their subsequent movement from one point to another.

57. **Alternative remittance systems (ARS)** are not necessarily illegal, and these systems often serve as a convenient and easily accessible means of transfer for communities that do not have easy access to traditional financial transfer services. However, due to the extensive anonymity built into **SARs,** these systems are misused to transfer illicit proceeds and therefore represent a serious **anti-TF/PF** challenge for regulators and **LEAs**.

58. **FIUs** face the challenge that, under regular circumstances, it is very difficult to detect hawala-linked transfers based solely on information gathered through **SARs.** Often, additional information from multiple sources is necessary to establish that the persons or entities involved are operating a hawala system. Nevertheless, **FIUs** are strategically positioned to detect potential hawala activities. While most Customs Services do not have a specific mandate to pursue illicit electronic funds transfers, they are uniquely positioned to intercept contraband currency and currency equivalents (gems and precious metals) and detect hawala systems using couriers.

59. Key practical recommendations for Customs and its officers to address these criminal activities include:

- *Customs and **FIU** should establish basic training and other training activities for officers and agents at the border to promote general awareness of **MVTS** activities. This training should include specific guidance on what to look for when confronted with possible currency smuggling related to this criminal phenomenon.*

- ***FIUs** and Customs Services should collaborate, in accordance with their respective legal frameworks of competence and in line with the general principle of operational independence and autonomy to identify the use of **MVTS** services and hawala systems in **TF/PF** related activities.*

2.2.4. FREE TRADE ZONES (FTA)

60. **Free Trade Zones (FTZs)** are defined areas within a country into which goods can be imported or entered, handled, processed, assembled, manufactured or reconfigured and re-exported, with a variety of benefits for the companies involved in such businesses. Such benefits include tax exemptions, simplified administrative processes and the export of raw materials, machinery, parts and equipment free of duties. **FTZs** are generally located near major ports, international airports and national borders, or places that offer geographical advantages for the commercialization of the goods in question.

61. The report prepared in 2010 by the **Financial Action Task Force (FATF)** on laundering in free trade zones[6] **(FTA)** states in one of its case studies that some criminal structures operating in various parts of the world including Central and South America carried out laundering based on foreign trade operations (**Trade Based Money Laundering, TBML, for its acronym in English**) related to **FT.** These operations are one of the modalities chosen by criminal groups and terrorist organizations to launder funds of illicit origin by exploiting the international trade system for the purpose of transferring goods and securities, while concealing the true illicit origin of those resources.

62. The misuse of **FTZs** affects all jurisdictions, including those countries where there are no **FTZs,** as goods may originate or be transshipped to multiple destinations through an area that is not subject to adequate export controls. In most cases, **TBML** activities involve conduct intended to distort the price of the subject merchandise through the use of a variety of methods to operate, such as under-invoicing, over-invoicing, multiple invoicing, shipping at values above or below the amounts shown on commercial documents, altering quality, falsely describing goods, and altering the quantity of goods as they move across borders or through supply chains. This masking process varies in complexity, depending on a variety of factors. **FTAs** can also be used to create legal entities and access the international financial system, providing opportunities to give the appearance of legality to illicit goods. Many of these zones are located in regional financial centers.

63. In this way, FTZs have enormous potential to be misused by criminal organizations, terrorist groups and proliferator networks to exploit the international trade system with a relatively low risk of detection. According to the FATF, the main vulnerabilities are as follows:

- *High volume of trade flows, which overshadow individual transactions and provide multiple opportunities for criminal organizations to transfer value across borders.*
- *Complexity associated with currency transactions (often multiple) and alternatives to various financial arrangements.*

6. Case Study No.2, Pg. 21, https://www.fatf-gafi.org/media/fatf/documents/reports/ML%20vulnerabilities%20of%20Free%20Trade%20Zones.pdf

- *Additional complexity that may arise from the practice of entering illicit funds with the cash flows of legitimate businesses.*
- *Limited scope of verification procedures or programs for the exchange of customs data between countries;*
- *Inadequate systems of customs agencies to detect illegal trade transactions.*
- *Lack of adequacy of substantive and procedural legislative norms that allow for an efficient mechanism for the prosecution of crimes related to ML and/or FT/FP.*

MEXICO

*In October 2020, the **Financial Intelligence Unit (UIF)** signed an agreement with the Ministry of Finance and Public Credit **(SHCP)** and the Confederation of Customs Agents Associations of the Mexican Republic **(CAAAREM).** The main objective of this agreement is to combat crimes involving operations with resources of illicit origin and the financing of terrorism and to identify these criminal activities in the exercise of foreign trade. Among the activities included in the agreement is the design and implementation of best practices in preventive matters, as well as the organization of roundtables and working groups, forums, workshops and seminars to promote a culture of legality.*

SPAIN

*In 2018, the National Police and the Civil Guard with the collaboration of the Tax Agency (Customs) dismantled several networks specialized in the trade and smuggling of defense and dual-use materials related to **WMD** proliferation. A number of cases under investigation related to the evasion of **FP** sanctions benefited from the collaboration of different authorities, including **SEPBLAC.** In addition, in order to facilitate cooperation with **LEAs** on **FP** matters, **SEPBLAC** incorporated personnel from the National Police Corps and the Civil Guard with experience in counter-proliferation related investigations and as a result of this action a number of cases have been processed and investigations improved.*

WCO - INTERPOL: "OPERATION TENTACLE".

*From August 26 to October 6, 2019, an operational effort was conducted in Asia-Pacific with the support of the 19 customs services involved and **INTERPOL's** Financial Crimes Unit leading to the seizure and arrest of more than USD 5 million in a combination of currency and gold smuggled across international borders. The operation resulted in the arrest of 14 suspected criminals linked to **LA.** The success of Operation Tentacle Asia-Pacific led to the establishment of Project Tentacle, to combat **LA** and **FT** in the customs environment. The Project is an initiative led by the **WCO** Secretariat and aimed at combating bulk cash smuggling and smuggling of gems and precious metals. In addition, the Project places emphasis on the advancement of **LA** and **TF** investigations following seizure at the border, as well as collaboration between Customs and **FIUs** and law enforcement. Project Tentacle enhances regional security through capacity building, and intelligence sharing between Customs, **FIU** and LEA. It not only aims to enhance Customs' capabilities by providing training in detection and investigative techniques, but also strengthens members' capabilities in financial crime intelligence and operational planning*

2.3. GOOD PRACTICES WITHIN THE FRAMEWORK OF NATIONAL CTF/CPF COOPERATION MECHANISMS

***a.** FIUs should be authorized to obtain (in the modes of receiving, obtaining and/or accessing) information held by all competent national law enforcement authorities, including the police, customs authorities, tax authorities, immigration, anti-drug agencies, anti-corruption agencies and intelligence services.*

64. **FATF Recommendation 29** and its related Interpretative Note do not detail the law enforcement agencies from which **FIUs** should be able to collect information. However, it seems logical that the criteria for including a particular **LEA** on such a list would depend on:

- *Whether the **LEA** is responsible for investigating **LA**, predicate offenses or **FT/FP** related offenses.*
- *Whether the **LEA** has data relevant to the work of the **FIU.***

65. While it is understandable that not all existing **LEAs** should be included in this list, providing specific examples of **LEAs** could be useful for those jurisdictions facing problems in this regard. These examples should take into account the fact that, in most countries, **LEAs** are responsible for dealing with tax-related offenses and other types of fraud, corruption, trafficking in persons and terrorism (i.e., offenses that are also relevant from the perspective of the **FIU's** remit).

***b.** FIU access to national LEA information should not be subject to a mandatory Memorandum of Understanding (MOU).*

66. In practice, most **MOUs** facilitate solutions with respect to the technical aspects of cooperation between **FIUs** and **LEAs** and allow **FIUs** to request information from **LEAs** without requiring a legal justification for each individual request. However, in most jurisdictions, these **MOUs** are not mandatory, but rather policy statements regarding access to information.

***c.** FIUs should have direct access to all relevant information maintained by LEAs. Where this is not possible due to technical reasons (such as incompatibility of IT systems, lack of an integrated database or the LEA's data storage manual), FIUs should be allowed to receive relevant information within a reasonable timeframe. In urgent cases, the deadline for receiving information from the LEA should be reduced.*

67. **FATF Recommendation 29** and its Interpretative Note stipulate that **FIUs** should have timely access to **LEA** information required to carry out their functions. However, in some jurisdictions, the time required to receive responses from **LEAs** does not meet this requirement. While **FIUs** have the power to suspend/postpone suspicious transactions for a certain, usually short, period of time, however, it is difficult to imagine how, in such urgent cases, **FIUs** can practically and effectively exercise their power to suspend transactions without having access to at least the suspect's criminal history information.

***d.** FIUs should have access to all relevant information maintained by LEAs, including information on investigations, prosecutions and convictions, and criminal history information.*

68. **FATF Recommendation 29 a**nd its Interpretative Note do not specify the type of information that **FIUs** should be able to obtain from **LEAs.** However, the following wording is used to address this issue: "information they need to carry out their functions". Notwithstanding this, it is significant that globally a large number of **FIUs** do not have access to the following data:

- *Operational information*
- *Mutual legal assistance data*
- *Information on persons investigated and/or convicted of committing an administrative offense*
- *Data maintained by Interpol*
- *Information on documents and/or other evidence seized and analyzed*
- *Data on modus operandi*
- *Information on the results of the financial investigation of predicate offenses*
- *Data on the amount of suspicious income generated by criminal offenses*
- *Tax information*
- *Immigration information*
- *Customs information*

***e.** When an FIU requests or accesses information from LEAs on behalf of a foreign FIU, restrictive conditions, such as the need for an MLA request or MOU, should not apply.*

69. **FATF Recommendation 40** and its Interpretative Note require **FIUs** to have the power to exchange:

- *All information required to be accessible or obtainable directly or indirectly by the **FIU** under the **FATF Recommendations, in particular Recommendation 29; and***
- *Any other information that they have the power to obtain or access, directly or indirectly, at the national level, subject to the principle of reciprocity.*

70. While seeking the consent of the **LEA** providing information seems logical, because the **LEA** owns the information, requiring an **MLA** request or the signing of a prior **MOU** in such cases creates unnecessary barriers that could prevent the timely exchange of information.

***f.** FIUs should be authorized to disseminate their information to the competent national authorities when their analysis shows that there is no suspicion of ML, associated predicate offenses or FT/FP, but they have reason to suspect that:*

- *Other crimes (at least serious) were committed; or*
- *Administrative infractions related to non-compliance with **CTF/CPF** legislation were committed.*

71. **FATF Recommendation 20** requires obliged entities to inform the **FIU** when they suspect or have reasonable grounds to suspect that funds are the proceeds of crime, or are related to **FT/FP**. This means that **FIUs** are receiving **STRs** related to any crime, including those where the perpetrators have only attempted to commit a crime and where there is no suspicion of **ML** and/or **FT/FP.** It stands to reason that in such cases, where the **FIU** analysis shows that there is a suspicion that the funds are proceeds of crime, **FIUs** should be authorized to report their findings to the competent **LEAs** in accordance with international standards for the protection of personal data.

***g.** The legislation should clearly identify the recipients of information and/or FIU reports containing confidential data.*

72. **FIU** information, and in particular analytical reports, almost always contain data that falls under state control, official, bank secrecy or other professional secrecy. Therefore, the **FATF** Interpretative Note to **Recommendation 29** requires that information received, processed, retained or disseminated by the **FIU** should be securely protected, and exchanged and used only in accordance with applicable procedures, policies, laws and regulations.

***h.**The legal status of FIU information disseminated to LEAs and/or other competent authorities should be regulated in national legislation. In designing their legal systems, countries should consider all the advantages and disadvantages of the different existing regimes with respect to the legal status of FIU information.*

73. In most jurisdictions, **FIU** information and reports can only be used by the recipient as intelligence, thus following minimum international standards. In some jurisdictions, **FIU** information and documents may be used as evidence in criminal proceedings and this depends on the content of the information and/or the recipient of the information. **LEAs** may use **FIU** information and reports as intelligence and in some scenarios as evidence, depending on the content of the information (e.g., whether the **FIU** information relates to **ML/TF/TF/PF** or only to other criminal offenses).

i. ***The legislation should specify the conditions that allow for the withdrawal of confidentiality of FIU information when necessary.***

74. The **FATF** Interpretative Note to **Recommendation 29** invites countries to adopt the necessary rules and procedures to enable the confidentiality of **FIU** information and reports to be withdrawn. However, in a large number of jurisdictions, legislation requires that **FIU** information disseminated to **LEAs** be treated as confidential. Interestingly, however, in most cases, **FIUs** do not have specific regulations on the conditions that would allow confidentiality to be withdrawn.

j. ***Competent LEAs should be able to request all relevant information held by the FIU when conducting investigations of ML, associated predicate offenses and FT/FP.***

75. This recommendation strictly follows **FATF Recommendation 31**, which regulates the right of competent **LEAs** to request relevant information held by the **FIU** when conducting investigations of **ML**, predicate offenses and **FT/FP.**

k. ***The LEA's request for information held by the FIU should explain the background to the request and, at a minimum, the following information should be included in the request:***

- *Legal basis*
- *Description of a case (including what triggered the **LEA's** interest in a particular case/individual), and*
- *Reasons for suspicion of **LA, predicate offenses and/or FT/FP***

76. In most jurisdictions, **LEAs** must explain the background of their request to the **FIU** so that the **FIU** can assess whether the **LEA's** request for information meets the criteria contained in **FATF Recommendation 31 (e.g., that the case relates to ML, predicate offenses and/or FT/FP)**. A similar requirement exists within the **Egmont Group** in relation to requests for information from **FIUs.**

l. ***There should be an explicit legal and/or statutory basis in national legislation that defines the power of LEAs and other competent authorities to request information from the FIU, clearly identifies the competent authorities and specifies the conditions that have to be met before such requests are sent.***

77. **FATF Recommendation 31** requires **LEAs** and other competent authorities to request all information held by the **FIU** when conducting investigations of **ML** or predicate offenses, and/or **FT/FP.** Therefore, at a minimum, it is expected that, if countries allow their **LEAs** to request data from **FIUs** on the basis of other circumstances, this should be clearly regulated in legislation and set out the conditions that must be met before such requests are sent.

m. ***The conditions under which the FIU may conduct analysis and disseminate information to LEAs or other competent authorities based on its request should be regulated in the legislation.***

78. **FIUs** have unique powers that are not granted to **LEAs** or other competent authorities and should be able to use these powers only in strictly regulated circumstances. There are a number of circumstances and conditions, which should be considered by all countries:

- *Suspected **LA / FT.***
- *Suspected felony / predicate offense and/or **FT/FP.***
- *Minimum requirements regarding the content of the application.*
- *The applicant authority must be one of the authorities explicitly mentioned.*
- *The application must be based on the international exchange of information.*
- *The request must not relate to a case that is already subject to prosecution under criminal law.*

n. ***The FIU should decide on the priority of incoming information/requests from the LEA depending on the purpose and/or circumstances related to the case.***

79. According to **FATF Recommendation 29** and the related Interpretative Note, **FIUs** should serve as a hub for the receipt and analysis of information from reporting entities and other information relevant to **ML,** predicate offenses and/or **FT/FP,** and for the dissemination of the results of their analysis to **LEAs** and other competent authorities. The same standard, and most country practices, also require **FIUs** to respond to requests for information from competent authorities if certain conditions are met. Based on these and other inputs **(such as requests received from foreign FIUs), FIUs** should be able to decide independently on the priority of incoming information/requests taking into account the purpose and/or circumstances related to the case.

o. ***Where LEAs request information from FIUs on behalf of a foreign LEA, there should not be excessive or unduly limiting restrictions. The same conditions should apply as for mutual legal assistance requests or requests sent through a foreign FIU.***

80. **FATF Recommendation 40** and its Interpretative Note require countries to allow their competent authorities to exchange information directly with their counterparts and even encourages allowing the rapid and smooth exchange of information directly with

non-counterpart agencies and entities. It is clear from this statement that **FIUs** should be able to respond to requests received from **LEAs** on behalf of foreign **LEAs** when certain conditions are met (e.g., the request is related to ML, associated predicate offenses and **FT/FP,** and the requested assistance does not impede an ongoing inquiry, investigation or proceeding). Advising the requesting foreign authority to use the **MLA** or **FIU** channels in such cases would undoubtedly cause delays in providing assistance and may be unduly restrictive. Therefore, requiring the foreign **LEA** to inform its **FIU** before sending such a request through **LEA** channels would certainly be advisable.

p. ***Direct access by the LEA to FIU data and/or information, if permitted, should be regulated in legislation. When deciding on the type of data and/or information to which LEA may have direct access, countries should take into account international requirements related to the operational independence of FIUs, as well as the security and confidentiality of data and/or information.***

81. A significant number of **LEAs** have access to foreign exchange transaction reports, cross-border cash and bearer instrument reports, wire transfer reports, **SARs** and analytical reports. International standards regulate the **FIU's** mandate, functions, access to information, information security, and confidentiality, **Egmont** membership and international cooperation. They also require countries to ensure that **FIUs** are operationally independent and autonomous, including when information must be sent or disseminated to competent authorities. In addition, **FATF Recommendation 31** clearly determines when **LEAs** or other competent authorities may request information from the **FIU**. The recommendation recognizes the fact that the **FATF** standards mentioned above do not explicitly regulate direct access by **LEAs** to **FIU** information. However, it also invites countries to consider these standards when making arrangements that may adversely affect the operational independence of **FIUs** and their obligation to protect the confidentiality of data. While there are some arguments supporting **LEA** access to foreign exchange transaction reports, reports on cross-border transportation of cash or bearer instruments, wire transfer reports, direct access by **LEAs** to **SARs** and analytical reports of the **FIU** may come to be seen as problematic in terms of the operational independence of **FIUs** and the security and confidentiality of data. In any event, it is unacceptable that direct **LEA** access to **FIU** data, if permitted, is not regulated in legislation.

q. ***LEAs and other recipients of FIU information should provide adequate, appropriate and timely feedback to the FIU on the use of the information. In this regard, an acknowledgement by LEAs of receipt of information from the FIU is not considered sufficient. The obligation to provide feedback may be a legal requirement or may depend on other forms of cooperation between FIUs and recipients of their information (e.g. MOUs).***

82. Most **FIUs** receive feedback from **LEAs** on the use of their information. In some jurisdictions, providing feedback to the **FIU** is a legal obligation while in other jurisdictions providing feedback is not a legal requirement. With respect to the type of feedback, a large majority of **FIUs** receive "targeted feedback" (i.e., information is provided on a "case by case" basis) as well as "general feedback". The **FATF** regulates feedback in **Recommendation 34,** however, this recommendation only requires authorities and supervisors to provide feedback (and guidance) to financial institutions and other regulated entities. Nevertheless, the **FATF** in Immediate Outcome 6 requires a measure of the effectiveness of the **FIU's** work and the extent to which analysis and dissemination is supporting the operational needs of competent authorities. Appropriate and timely feedback to the **FIU** is one of the key tools employed to meet the requirements of this standard. Acknowledgement by **LEAs** of the receipt of information from the **FIU,** while useful, cannot fulfill the above purpose.

2.4. NATIONAL FRAMEWORKS FOR INTER-INSTITUTIONAL COOPERATION AND COORDINATION

83. The way in which a country organizes its national framework for coordination and cooperation in **CTF/CPF** matters will have an impact on the implementation of mechanisms and procedures for the prevention, investigation, disruption and repression of **TF/ PF**.

84. The characteristics of an effective **CTF/CPF** inter-institutional cooperation system generally include:

- *Involvement of all relevant agencies at the political, legal and operational levels, as well as at the national and regional levels;*
- *Presence of a lead agency/body/committee and an established coordination mechanism backed by a high level of political will (e.g. ministerial level mandate) and responsible for policy formulation, prioritizing policy programs in the **TF/PF** context, making appointments, etc...;*
- *Designation of the appropriate level of decision making officers for other relevant agencies involved in interagency activities;*
- *Conduct regular and ad hoc meetings, as well as periodic training sessions to enable the exchange of information on latest supervisory and compliance experiences, feedback on suspicious transactions, progress in investigation and prosecution, follow-up on supervisory actions, latest typologies, evasion methods, statistics related to proliferation financing (e.g., amount of assets seized);*
- *The competent authorities have the necessary legal powers to allow the exchange of information (e.g., intelligence, financial intelligence or suspicious transaction reports) and to conduct joint investigations. In some cases, a memorandum of understanding or a policy memorandum is prepared to clarify specific operational procedures;*

- *Establishment of operational procedures or a response mechanism on how the respective competent authorities should handle investigations related to freezing measures, false positives, possible evasions;*

- *Adoption of a uniform approach to engagement and outreach, including the frequency and content of materials to be shared with the private sector; and*

- *Use of formal and informal communication and cooperation channels.*

3. CTF/CPF COORDINATING COMMITTEE OR AGENCY

85. The role of the lead agency or committee within the framework of the **CTF/CPF** fight should include the exercise of the following functions within its scope of competence:

- *Ensure that the legal and regulatory framework is consistent with the latest requirements of the **UNSCRs** and the **FATF Recommendations** on targeted financial sanctions **(TFS) for TF/PF;***
- *Disseminate the requirements for the implementation of the **TFS** regime and **UNSC** obligations to government agencies, other relevant authorities and private sector stakeholders;*

- *Update government agencies, other competent authorities and private sector stakeholders on recent cases and typologies of **TF/PF**, where appropriate;*

- *Identify the agencies that should be involved in the exchange of information in **TF/PF** cases;*

- *Promote information sharing among different agencies to help identify **TF/PF** cases and prevent **TFS** evasion;*

- *Utilize a coordination platform/working group, periodic issuance of circulars, or establishment of a hotline to ensure that the various agencies understand their respective roles and oversight responsibilities, and respond to agency operational inquiries; and*

- *Ensure coordinated communication with the private sector to enable consistency in messages/requirements/obligations/communications, especially when more than one government agency and/or department is involved in such communication.*

COLOMBIA

*The Coordination Center against the Finances of Transnational Crime Organizations and Terrorism was created by means of Law 1941 of 2018, as a permanent instance with the objective of pursuing and dismantling the networks of money and goods of illicit origin or used in illicit activities, money laundering and financing of terrorism, through the joint and coordinated work of the Public Force, the agencies that carry out intelligence and counterintelligence activities, the Attorney General's Office and the judicial authorities, within the framework of each of their competencies. Likewise, it was established that the Technical Secretariat of the Center will be exercised by the Information and Financial Analysis Unit, **UIAF**. Interadministrative Cooperation Agreement. On November 30, 2015, an Interadministrative Cooperation Agreement was signed between the Ministry of Foreign Affairs, the Information and Financial Analysis Unit UIAF, the Financial Superintendence of Colombia and the Attorney General's Office, whose purpose is to comply with international obligations on freezing and prohibition of handling funds or other assets of persons and entities associated with terrorist acts or groups assumed by Colombia, especially Resolutions 1267 of 1999, 1988 of 2011, 1373 of 2001, 1718 and 1737 of 2006 of the United Nations Security Council -CSNU- and Recommendations 6 and 7 of the FATF.*

SPAIN

*On January 22, 2018, Spain created a Specialized Committee on Non-Proliferation of Weapons of Mass Destruction by Ministerial Order /29/2018. It is a support body to the National Security Council and provides a coordination mechanism for national authorities involved in proliferation matters, including the Secretariat of the AML Commission. The Committee meets every two months to coordinate the positions of its members with respect to the development and implementation of national nonproliferation policies, but may meet more frequently as needed. In addition, to facilitate the identification and disruption of instances of proliferation and misuse of defense or dual-use materials, this Committee created an operational working group called the Interdiction Working Group. The Interdiction Working Group is configured to provide a coordinated operational response to instances of potential violation of the **WMD** non-proliferation regime by facilitating the exchange of financial and other sensitive information between law enforcement, intelligence services and, in particular, SEPBLAC (FIU). Members of the Interdiction Working Group have cooperated bilaterally in identifying cases of possible PF TFS evasion.*

BELGIUM

*Belgium has a national coordinating authority for assessing **LA** risks and another authority for assessing **TF** risks. Due to the sensitivity of terrorism and **TF** issues, Belgian legislators decided to delegate the coordination of the fight against **LA** to a coordinating body, and against **TF** to a separate body, each composed of different stakeholders. In Belgium, the **TF** Committee was integrated into the National Security Committee, because issues related to terrorism and terrorist financing can be complementary*

*and often involve the same people. Terrorist financing risk assessment is the responsibility of the committee in charge of coordinating the fight against terrorist financing. The National Security Council deals with terrorism and security issues and, since 2013, also deals with **TF/PF** issues. The Strategic Intelligence and Security Committee and the Intelligence Service implement the decisions of the National Security Council. A specific TF platform within the Intelligence Service and a Security Coordination Committee were created to address TF issues.*

ITALY

*Italy has a strategic committee for combating terrorism, which is also responsible for handling matters related to the fight against terrorist financing, and which delegated the preparation from the terrorist financing risk assessment to a dedicated group of experts. The Financial Security Committee is the national body involved in the fight against TF that is responsible for conducting and updating the national risk assessment. The committee has been established as part of the Italian Ministry of Economy and Finance and has been entrusted with the task of coordinating actions for the prevention of the use of the financial system and the economy for **LA, FT/FP** related purposes. The Financial Security Committee is made up of key competent authorities. Its composition has been supplemented by additional representatives of the participating authorities in relation to the specific issues discussed. The Committee established an ad hoc working group to develop a proposal for the method of analysis and to conduct the assessment. The key competent authorities may share any information among themselves and are exempt from all applicable rules on official secrecy. All information acquired by the committee is covered by official secrecy. The judicial authorities will forward to the committee any information it deems useful for its purposes.*

The Chairman of the Committee may transmit data and information to the Executive, the Intelligence Committee and the Security Services and to the heads of intelligence and security services for coordination activities under the responsibility of the Prime Minister.

AUSTRALIA

*Australia has a wide range of mechanisms for coordination and cooperation in the fight against **ML** and **TF** at both the policy and operational levels. The main federal coordinating body is the Interdepartmental Anti-Money Laundering Committee. Committee, which meets to share information and inform the strategic direction and priority setting of federal agencies working on national initiatives to counter **LA** and **TF.***

Activities related to anti-money laundering and combating the financing of terrorism are also coordinated through the National Organized Crime Response Plan and other interdepartmental law enforcement agencies.

***TF** policy is coordinated by the Interdepartmental Committee. Operational matters are coordinated through the various agencies responsible for **TF** investigation. The Interdepartmental Committee uses the national risk assessment to establish annual risk-based priorities to guide the work and resource allocation of its member agencies on matters related to combating **LA** and **TF**. In September 2012, the states and territories of the Commonwealth governments, entered into a formal agreement to include New Zealand as a member of the so-called Australia-New Zealand Counter Terrorism Committee. Previously, New Zealand had only observer status in the Australian National Counter Terrorism Committee. The Australia-New Zealand Counter-Terrorism Committee is a high-level bilateral intergovernmental committee to coordinate counter-terrorism capabilities. The Committee builds on strong cooperation between the two countries and established capabilities in areas such as crisis management, command and control, intelligence and investigation, and media cooperation.*

3.1. JOINT INVESTIGATION TEAMS

86. **Joint investigation teams (JITs)** make it possible for agencies with common interests to work together on an investigation. In addition to sharing information, it allows an investigation team to make use of a wider range of skills and experiences of investigators with different backgrounds and training. Joint investigations have the potential to avoid duplication arising from parallel investigations and to increase efficiency by making it possible for staff members from each agency to focus on different aspects of an investigation depending on their professional experience and technical expertise. In some cases, information sharing portals are more extensive when agencies are involved in a joint investigation than they otherwise would be.

Countries using these strategies include Australia, Austria, Canada, Denmark, Finland, India, Japan, Luxembourg, the Netherlands, Portugal, Slovenia, South Africa, Spain, Turkey, the United States, India, and the Netherlands.

3.2. INTER-AGENCY INTELLIGENCE CENTERS

87. Interagency intelligence centers are typically established to centralize the processes of obtaining and analyzing information for a number of agencies. The focus may be on a specific geographic area or type of criminal activity or have a broader role in information sharing. These centers conduct analysis based on primary research as well as information obtained from agencies. In some cases they access data through portals available to participating agencies, while in other cases they have specific information-gathering powers. By centralizing these activities, a center's staff members gain expertise on particular legal and practical issues and specialized systems can be created that can increase their efficiency. Cost savings can also be achieved by sharing the expense of obtaining, processing and analyzing data among the participating agencies.

> *Countries using these strategies include Australia, Finland, India, the Netherlands, Sweden, the United States and the United States.*

3.3. SERVICE MISSIONS AND CO-LOCATION OF PERSONNEL

88. Secondments and co-location of staff are effective ways of enabling the transfer of skills while allowing staff to network with their counterparts in other agencies. Seconded staff members share their skills, experience and specialized knowledge while at the same time participating directly in the work of the host agency. Countries report that co-location and secondment arrangements have wider benefits for interagency cooperation by encouraging staff to be more proactive in building relationships with their counterparts in other agencies and improving the effectiveness of the collaboration that is achieved.

> *Countries using these strategies include Australia, Belgium, Canada, Finland, France, Ireland, Italy, Japan, Korea, the Netherlands, Norway, Spain, the United Kingdom, the United States and the United States.*

3.4 OTHER PRACTICES

89. Other strategies include the use of shared databases, the dissemination of strategic intelligence products such as intelligence bulletins and briefs, joint committees to coordinate policy in areas of shared responsibility, and interagency meetings and training sessions to share information on **TF/PF** trends, guidance on investigative techniques and best practices in case management.

> *Countries using these strategies include Australia, Austria, Canada, the Czech Republic, Finland, India, Ireland, Italy, Japan, Luxembourg, the Netherlands, New Zealand, the Slovak Republic, South Africa, Turkey, the United States and the United Kingdom.*

CHAPTER II

STRATEGIC PROCEDURES FOR DETECTION, INVESTIGATION AND DISRUPTION OF FT/FP

1. INTRODUCTION

90. While financial institutions, supervisory and regulatory agencies and the private sector play a critical role in preventing **TF/PF**, there is unanimous agreement that for global **CTF/CFP** efforts to be effective and efficient, countries must have a strong institutional, legal and procedural framework in place to conduct analysis and investigations, initiate prosecutions, and obtain convictions. Investigating and sanctioning **TF/PF** cases presents a different set of challenges for national jurisdictions. **TF/PF** cases often involve classified intelligence, can span multiple jurisdictions, and require swift responses from investigators and judicial authorities to combat **WMD** proliferation and terrorist financing networks that constantly change their methods of operation to avoid interdiction.

91. As can be seen from the Fourth Round Mutual Evaluation Reports conducted on the basis of the 2013 methodology, many countries have enacted the necessary legislative measures to criminalize **ML** and **FT**, however, the results obtained in terms of convictions and confiscations are modest overall. Achieving results in this area in the framework of the **CTF/CFP** fight represents a serious problem for prosecutors, judges and investigators and other actors part of the criminal justice system. From the initiation of a criminal investigation to the criminal conviction of a defendant, the justice system can involve many government actors with different roles that need to coordinate with each other.

92. The proper functioning of criminal justice systems in the region based on stable institutions governed by the principles of accountability, integrity, transparency and the rule of law are essential pillars of a comprehensive system to combat **CTF/CPF.** The Codes of Criminal Procedure and administrative punitive regulations of the countries of the hemisphere must be modified to implement a comprehensive system for investigating and punishing **FT/CFP**, since in addition to the lack of criminalization of these criminal conducts, the lack of specialization of judges and prosecutors in these matters is a serious concern. The absence of special procedures for the prosecution of these criminal activities and the lack of criminal liability of legal persons in many legislations have been identified as two of the main challenges for prosecuting this type of crime.

2. FT/FP INDICATORS

2.1. FT INDICATORS

93. The indicators for detecting whether **TF** is occurring can be classified as follows:

i). Indicators relating to individuals

- *With regard to financial activity, the following indicators are identified for monitoring:*

i. *Misuse of social benefits or suspicious tax refund claims.*

ii. *Receipt of financial support (or expenses and assets paid) from an unforeseen or undefined source.*

iii. *Transfers of funds to or from hostile or war zones or neighboring regions.*

iv. *ATM transactions in conflict zones or neighboring regions.*

v. *Movement of funds unrelated to employment or other financial arrangements.*

vi. *Credit cards that are reaching or have reached their limit as a result of cash withdrawals.*

vii. *Accumulation of loans obtained from various suppliers, in a short period of time, with possible default on repayments.*

viii. *Payments for travel to and from hostile or conflict zones or neighboring regions.*

ix. *Significant or frequent donations to charitable organizations that are related to conflict zones or neighboring regions.*

x. *Payments to media or bookstores associated with the propagation of radicalism, extremism or violence (e.g., for consumption or creation of propaganda materials, printers, leaflets, banners, etc.).*

xi. *Change in the use of money, such as, for example, a sudden use of less transparent financial instruments.*

xii. *Use of wire transfers to or from risk countries or between individuals located in the same jurisdiction, for amounts below the threshold above which there is an obligation to declare, in order to avoid detection, or without a commercial purpose.*

xiii. *Power of attorney related to a third party's bank account.*

xiv. *Loans granted to individuals without any commercial purpose (generally without repayments).*

xv. *Donation of funds to known extremist entities.*

xvi. *Misuse of encrypted money transfer applications (e.g., through payments made via mobile messaging applications).*

xvii. *Accumulation of funds from various sources in a single account with movement to a single receiving account (e.g., it could be a potential agent), either domestic or foreign.*

xviii. *Loan agreements, lines of credit or credit card loans with no repayments.*

xix. *Use of one or more shell companies.*

xx. *Purchase or sale of high-value goods (e.g., cultural property) from conflict zones or neighboring regions.*

xxi. *Purchase or sale of counterfeit goods.*

xxii. *Numerous loan applications.*

xxiii. *High volume of cash deposits exceeding declared or known sources, particularly in personal accounts.*

xxiv. *Deposit transactions carried out at a location that is a great geographical distance from where the accounts or account holders are domiciled.*

xxv. *Unexpected amounts of cash in commercial premises or in the domestic residence.*

xxvi. *Transfer or disbursement of funds shortly after making cash deposits.*

- *In terms of personal behavior, the following indicators stand out:*

i. *Radicalization (e.g., adoption of a name related to extremist or fundamentalist groups or movements, sudden break with usual lifestyle or behavior, conservative religious dress, etc.).*

ii. *Exhibition of extremist political or religious views that incite the use of violence.*

iii. *Criticism of the government or government policies regarding issues related to combating terrorism; processes of radicalization, extremism or violence (e.g., attitude observed through the individual's use of social media).*

iv. *Travel to and from hostile or conflict zones or neighboring regions.*

v. *Inclusion of the person on a sanctions list*

vi. *Inclusion in a client list of tax advisors or accountants participating in illicit refund programs.*

ii). Indicators related to companies

- *The following six indicators should be monitored for unusual economic operations and participants:*

i. *Transactions (e.g., remittances, wire transfers, money transfers, use of money carrier) with intervening parties located in conflict zones and nearby regions.*

ii. *Funds transfers outside regulated financial institutions (e.g., hawala and other informal funds transfer systems).*

iii. *Funds transfers made through encrypted money transfer applications (e.g., mobile messaging applications).*

iv. *Transactions with an unusual lender.*

v. *Suspicious or fictitious commercial reimbursements to customers who have already received them (a transaction that may indicate a movement of funds from a company to one or more individuals belonging to a terrorist cell).*

vi. *Risk assets, such as high-value, dual-use assets in unexpectedly large quantities.*

- *Regarding unusual cash flows:*

i. *Abundant flows of money into or out of the company's accounts with no apparent legitimate business purpose.*

ii. *Lack of documentation on the purpose, source or destination of funds.*

iii. *Transfer or disbursement of funds shortly after making cash deposits.*

iv. *Cash withdrawals in risk countries and at their borders.*

v. *High volume of cash deposits exceeding the declared or known sources.*

vi. *Deposit transactions carried out at a location that is a great geographical distance from where the accounts or account holders are domiciled.*

vii. *Indicators of other forms of fraud (e.g., credit cards, loans), such as a suspicious or unusual number of credit card or loan applications.*

viii. *Unexpected amounts of cash in commercial premises or in a residence.*

- *Regarding unusual commercial activity:*

i. *Purchase or storage of non-business-related assets (e.g., a printing company purchasing gas masks, encrypted telephones, camping equipment, fertilizer).*

ii. *Excessive purchase or storage of dual-use goods that are restricted or listed (e.g., radioactive material, chemicals and explosives).*

iii. *Unexplained inventory deficit of dual-use assets.*

iv. *Sale of dual-use goods that are restricted or listed to unknown or unauthorized buyers.*

v. *Excessive cash deposits and other holdings unrelated to sales or debt.*

vi. *Assets of the company used by unknown or unidentified individuals or entities, without remuneration.*

- *Regarding unusual expenses:*

i. *Payments for travel to and from conflict zones or neighboring regions, for another person.*

ii. *Significant or frequent donations to charitable organizations that have a relationship with conflict zones or neighboring regions.*

iii. *Assets paid by the company that cannot be located or verified.*

iv. *Invoices for advertising, publishing and printing expenses located or claimed, but not shown to be used by the company (may indicate the creation of advertising materials, such as printers, brochures, banners, etc.).*

v. *Assets or personal expenses paid by the company that do not appear to be used by the owner.*

iii). Indicators for charitable and non-profit organizations

- *With regard to unusual transactions and participants, it is advisable to monitor these indicators of possible terrorist financing:*

i. *Donations received from a State sponsor of terrorism or foreign entities located in or near a conflict zone, especially without any clear relationship or supporting documents.*

ii. *Donations for a significant total amount and not sufficiently justified, especially if they are made mainly in cash.*

iii. *Use of funds for expenses that are not related to the activity of nonprofit organizations.*

iv. *Transfers of money to jurisdictions that are not related to the areas of activity of charitable and non-profit organizations.*

v. *Actual expenditures on goods are different from those shown on invoices or shipping labels.*

vi. *The entity presents itself as a charitable organization, but operates in an unregistered capacity to avoid regulatory scrutiny.*

vii. *Directors, key employees or major donors who were previously involved with other suspect or sanctioned charities.*

viii. *Directors, key employees or major donors who are subject to adverse or negative information in the public domain.*

ix. *Foreign associated entities, agents or employees that are the subject of adverse or negative public information.*

x. *Transfer of funds or other assets to entities located in or operating in or near conflict zones, especially when there are no reported activities or programs in those zones.*

xi. *Association of directors, trustees, officers, key employees or agents of a charitable or non-profit organization with organizations or individuals of interest related to terrorism.*

xii. *Dissemination, distribution and publication of extremist ideologies or materials through the Internet or other media.*

iv) Indicators related to cryptocurrencies

- *As for the unusual origin:*

Receipt of cryptocurrencies from persons, entities or locations associated with terrorism or from conflict zones and neighboring regions.

- *Regarding unusual operations:*

i. *Transfer of cryptocurrencies or wallets to individuals or organizations linked to conflict zones and their neighboring regions.*

ii. *Cryptocurrency purchases of dual-use products, camping and survival equipment and medical supplies.*

iii. *Delivery of these cryptocurrency purchases targeted at conflict zones and their neighboring regions.*

2.2. PF INDICATORS

94. The identification of **FP** risk from **WMD** entails additional difficulties to the risk analysis in case of **TF** because most transactions occur within normal trade routes. The close relationship between safeguards against **TF** and export control systems entails some risks that should be avoided. Concurrence of responsibilities from both the export control side (exporters or export control authorities) and the financial side (banks or competent authorities, including FIUs) could lead to loss or duplication of efforts. Taking into account the specificities of international financial flows and the characteristics of international trade finance, it is not possible to expect from **FIUs** the same type of controls that are mandatory for exporters prior to the export of dual-use items listed in international export control regimes.

95. In some jurisdictions, competent authorities, including export control and customs agencies, may also use intelligence on potential suppliers or end-users of dual-use items linked to **WMD** programs when deciding whether to grant an export license or to allow the goods to pass through their borders. Other jurisdictions have developed profiles of suspect suppliers based on the commission of violations of export control provisions or end-users based on the application by customs authorities of the catch-all clause.

96. The main challenges include the following:

- *The purchase and sale of elementary components, as opposed to complete manufacturing systems. Individual elementary components may also have legitimate uses (dual-use goods), which makes their identification for illegitimate purposes even more problematic.*
- *Dual-use products are difficult to identify, require specialized knowledge and can be described in common terms with many uses.*
- *The networks through which proliferation-sensitive assets can be obtained tend to be complex. This, combined with the use of false documentation, allows the proliferation of sensitive goods, the entities involved, the associated financial transactions and the end user to avoid detection. Front companies, agents and other fake end users are often used to cover up for the end user.*
- ***TF** risk is more likely to exist in cases where the source of funds is legal and the end user of the type of goods involved is hidden, making it difficult to identify such activities.*
- ***PF** identification is not limited to persons and entities designated on sanctions lists and may involve other actors without an immediately obvious connection to the designated entities and persons, and disconnect from the physical flow of proliferation-sensitive goods.*
- *Detection is difficult because most transactions occur within normal business transaction routes and can be masked by all legitimate transactions.*
- *The general use of legal structures by organized criminal networks to conceal their proliferation activities. Because individuals involved in proliferation activities frequently use front men to establish companies, including legitimate companies that carry out such activities and mix illicit and licit funds, it is extremely important for authorities to have access to reliable, truthful and up-to-date information to identify the ultimate beneficiary of these structures, especially in cases linked to the designated non-financial business and professions **(DNFBP)** sector.*

97. The main indicators for detecting whether **WMD** proliferation financing is occurring can be classified as follows:

i). Customer-related indicators

- *The client is reluctant to provide additional information when requested.*
- *The customer's activity does not match the customer's business profile or the end user's information does not match the end user's business profile.*
- *The customer is a person or entity designated on the United Nations Security Council sanctions lists subject to or related to a designated person or entity.*
- *The customer is involved in the supply, sale, delivery or purchase of dual-use, proliferation-sensitive or military goods, particularly in higher risk jurisdictions.*
- *The customer or counterparty, or its address, is the same or similar to a party on publicly available lists or has a history of export control violations.*
- *The customer is a military or research organization related to a major risk.*
- *The new customer applies for a letter of credit from a bank, while waiting for account approval.*
- *The client uses a complex structure to hide involvement: use of layered letters of credit, front companies, intermediaries and brokers.*
- *The customer is a manufacturer or distributor of products subject to export controls.*
- *The customer or transaction counterparties are linked (e.g., they share a common physical address, IP address or telephone number, or their activities may be coordinated).*

ii). Transaction-related indicators

- *The transaction relates to dual-use, proliferation-sensitive or military goods, whether licensed or unlicensed.*
- *The transaction demonstrates a link between representatives of companies exchanging goods, e.g. same owners or management, in order to evade scrutiny of the exchanged goods.*
- *The transaction involves the shipment of goods that are not consistent with normal geographic trade patterns, i.e., where the country involved does not normally export or import the types of goods in question.*

- *The transaction involves persons or companies (in particular, trading companies) located in countries with weak export control laws or poor enforcement of export control laws.*
- *The transaction is carried out by companies with inconsistencies in the information contained in commercial documents and financial flows, e.g. names, addresses, final destination, etc.*
- *The transaction involves higher risk jurisdictions known to be involved in **WMD** proliferation or **PF** activities.*
- *The transaction involves potential shell companies (e.g., companies that do not have a high level of capitalization or show other indicators of shell companies).*
- *The transaction involves the participation of a small trading, brokerage or intermediary company (it may be conducting business inconsistent with its normal business).*
- *The transaction involves containers whose numbers have been changed or ships that have been renamed.*
- *The shipment of goods takes a circuit route or the financial transaction is structured as a circuit.*
- *The transaction involves the shipment of goods incompatible with the technical level of the country to which the goods are being shipped (e.g. semiconductor manufacturing equipment shipped to a country with no electronics industry).*
- *The goods are ordered by firms or individuals from foreign countries other than the country of the declared end use.*
- *The transaction involves financial institutions with known deficiencies in **AML/CFT** controls and/or domiciled in countries with weak export control laws or weak enforcement of export control laws.*
- *Unexplained timing differences with obviously connected transactions.*
- *Lack of counterparty information.*
- *Falta de información sobre contraparte.*
- *The transaction involves a **CFT**-listed State or a location near a **CFT**-listed State on the same terms.*
- *Uncertainty as to the final beneficiary and/or unidentified end user (e.g. a freight forwarder or a bank is listed as the final recipient or destination).*
- *Large volume transaction from a personal or diplomatic account.*

iii). Indicators related to documents

- *Evidence that documents or other representations relating to shipment, customs or payment are false or fraudulent (e.g. forged end-use certificates and forged export or re-export certificates).*
- *Declared value of shipment undervalued in relation to shipping cost.*
- *Trivial description in the customs declaration / export license, e.g. agriculture, electronics and pumps (without further explanation of purpose / use).*
- *Lack of documentation.*
- *Technical description altered.*
- *Inconsistencies in the information provided in trade documents and financial flows (e.g. names, companies, addresses, ports of call and final destination).*
- *Secondary data related to the target person (address, telephone number).*
- *Delivery ex works, i.e. the manufacturer is not responsible for shipping.*
- *Circular remittance route (if available) and/or circular financial transaction route;*
- *Final destination or end use unclear.*
- *The trade finance transaction involves a shipping route (if available) through a country with weak export control laws or poor enforcement of export control laws.*
- *Electronic instructions or payment of what is owed to entities not identified in the original letter of credit or other documentation.*
- *Pattern of wire transfer activity that shows unusual patterns or has no apparent purpose.*
- *Amounts below reporting thresholds in the context of multiple transactions.*
- *The description of the goods in the commercial or financial documentation is unspecific, innocuous or misleading.*

98. The presence of a single indicator may not automatically make a transaction suspicious. However, the combination of red flags with other indicators may warrant further investigation.

3. PARTICULARITIES IN FT/FP ANALYSIS AND RESEARCH

99. **TF/PF** cases often present difficulties in terms of gathering evidence linking the assets to criminal activities or proving that the funds are intended for terrorist purposes or linked to **WMD** proliferation. This linkage often has to be proven at trial and requires in-depth investigation due to the difficulty in proving it. To do so, analysts and investigators must identify and trace the assets or "follow the money" until the connection between the crime of terrorism, **WMD** proliferation and the assets linked to such criminal conduct can be established.

100. Justifying the existence of a nexus between a financial transaction and a terrorist and/or proliferation offense may also be essential for investigative measures such as search warrants, wiretap warrants and surveillance orders. It is imperative to be able to use circumstantial evidence, especially with respect to knowledge or purpose of the terrorist and/or **WMD** proliferation act.

101. In addressing the issue of evidence in **FT/FP** cases, a distinction must be made between direct and indirect evidence (or circumstantial evidence). Direct evidence is evidence that, if believed, establishes the existence of a particular fact without the need for any inference or presumption to connect the evidence to the fact. A clear example would be the direct testimony of a witness or a document showing that a particular person has a bank account. Indirect evidence relates to a fact or matter other than the particular fact sought to be proved. The party relying on it argues that indirect evidence is so intimately associated with the fact to be proved that it is possible for the fact to be proved to be inferred from the existence of the circumstantial. Therefore, indirect evidence requires that an inference be made to establish a fact. In other words, it does not point directly to a fact, but must be used to assemble a puzzle in order to reach an inference, which must be inescapable.

102. In **FT/FP** cases, there may be little, if any, direct evidence to demonstrate the source and/or destination of funds, so indirect or circumstantial evidence is particularly important. Of course, sometimes it will be possible to link a specific financial transaction directly to the alleged criminal conduct. Sometimes it will not. In those cases, in the absence of such a direct link, evidence of movements of money, assets, purchases or cash-based business transactions may, by itself or in conjunction with other evidence, allow an inference to be drawn that the funds in question are intended for terrorist purposes or linked to **WMD** proliferation.

3.1 INTELLIGENCE VS. EVIDENCE

103. Investigators capture information and interpret it to add value to the investigation. In many cases, intelligence is not presented in a form that satisfies the admissibility requirements that would allow it to be presented in court as relevant legal evidence. As a matter of good practice, it is important for investigators and prosecutors to have a clear view at an early stage of any challenges that may exist to ensure that investigative material can be admitted at trial and used as evidence, especially if it has been obtained from abroad. In some circumstances, sensitive documentation contains information that would harm a public interest or the security of the state or could compromise the safety of an individual. In such cases, careful consideration will need to be given to alternative ways of admitting the evidence in court.

104. Important points in intelligence gathering are:

- *Ensure that there is the legal power to collect the material and consider human rights principles;*
- *Ensure that sources and methodology are not compromised;*
- *Maintain adequate records of the authorization (court or superior officer), justification and execution of any covert or intrusive investigative methods.*
- *Ensure that the measures are proportionate, necessary and pursue a legitimate objective.*

105. Major challenges in **TF/PF** cases that relate to the availability and admissibility of evidence include:

- *Prove mens rea, i.e., that the defendant intended or knew that the funds were to be used by a terrorist, a terrorist group or for a terrorist act, or for purposes linked to **WMD** proliferation, especially when the defense claims that the funds were intended for personal expenses such as rent or food or charitable purposes.*
- *Demonstrate that the recipient of the funds or assets is a terrorist or terrorist organization or a network of **WMD** proliferators, especially if it has not been designated by the United Nations Security Council or national authorities.*
- *Verify the terrorist or proliferation-related purpose of **WMD** when funds are sent abroad, even if not used to finance a specific terrorist attack.*

106. There are particular challenges related to "converting" classified intelligence into admissible evidence:

- *The prosecution may have to find ways to recreate or corroborate information that would otherwise be found only in classified material.*
- *The prosecutor may find himself in a position where he would have to disclose secret information if he intended to prosecute, and could therefore refuse to file charges or dismiss the case.*
- *Sentences may be lower if all elements of TF/PF-related activity are not taken into account due to inadmissibility of evidence..*
- *Sentences may be lower if all elements of **FT/FP-related** activity are not taken into account due to inadmissibility of evidence.*
- *Onerous measures may be necessary to maintain the confidentiality of intelligence gathering resources and methods.*
- *Different people may have access to different levels of intelligence, such as the intelligence service, police or prosecutors, which can complicate cooperation between agencies.*

107. The following table presents a comparison between the advantages of using **FIU** information as intelligence and the advantages of using such information as evidence.

ADVANTAGES OF USING IFU INFORMATION AS INTELLIGENCE.	ADVANTAGES OF USING IFU INFORMATION AS EVIDENCE.
Promotes respect for due process, human and privacy rights, and evidence gathering procedures.	Saves time and resources of reporting entities, law enforcement agencies, prosecution and the courts.
Allows for a clear separation of the functions of the different bodies involved in criminal proceedings and pre-trial investigation.	Reduces the administrative burden for those entities that have already provided the information to the State authorities, while effectively protecting their identity.
Protect the source of suspicious transaction report **(STR)** / other information and maintain confidentiality throughout the process.	Facilitates and expedites investigation and prosecution, and avoids duplication of efforts.
Ensures better protection/security of the **FIU** and its staff, including preventing **FIU** staff from being subpoenaed to testify in court.	Allows tax and judicial authorities to benefit from the **FIU's** expertise (e.g., they can use the financial analysis and charts, hear testimony from **FIU** staff, etc.).
Allows a lower reporting threshold for the **FIU** to disseminate information. The **FIU** only needs to know what information is suspected to be relevant to the **LA** and/or **FT/FP.**	Not only does **FIU** information collected from foreign FIUs reach the judicial investigation faster when compared to mutual legal assistance channels, but given the extensive network of FIUs operating globally, it also allows information from foreign jurisdictions that would not otherwise be available to be obtained and utilized.
Allows for a wider range of information to be used, including unconfirmed information.	
Allows **FIU** information to be disseminated quickly because the **FIU** is not required to submit its information as evidence.	
FIU intelligence provides a lead to **LEAs** for investigation and facilitates their investigation by helping them focus on more important issues, thereby improving efficiency.	
FIU information is cross-checked, verified and supplemented with other related information before it can be used as evidence. Therefore, appropriate checks and balances are protected. information exchange.	
FIU information may also be used by competent **LEAs** to prevent **ML** and/or **FT/FP.**	
The **FIU** can disseminate information to a wide range of law enforcement agencies.	
FIU information can be easily exchanged with all types of foreign **FIUs**.	

108. Although gathering and using evidence is one of the most difficult tasks in **FT/FP** prosecutions, there are some good practices in this area:

- *Have legislation or judicial procedures that specifically address the use or introduction of classified material or intelligence (e.g., laws or regulations may allow prosecutors and/or defense attorneys to review information, the State may "declassify" information, etc.).*
- *Involve the prosecutor at an early stage to determine which pieces of intelligence can be admitted as evidence, or what steps should be taken to have them admitted.*
- *Conduct the investigation so that confidential intelligence is supplemented or supplanted by admissible evidence, such as financial records or communications records obtained by court authorization.*
- *Develop case law to allow the use of circumstantial and indirect evidence to prove knowledge and intent.*
- *Using the defendant's own words and activities, e.g., on social media, to help prove intent or to find witnesses who can testify regarding the defendant's behavior or beliefs and changes in beliefs.*
- *Implement the terrorism designations required by the United Nations and related designations and establish a system of national designations to assist in demonstrating that a person is a terrorist or that an organization is a terrorist organization, or develop case law that gives weight to foreign designations.*
- *Utilize the 24/7 electronic evidence system under Article 35 of the Budapest Convention[7] on cybercrime to obtain and provide immediate assistance in connection with the collection of electronic evidence.*
- *Have a special court designated to deal with terrorism and **FT/FP** cases that generally involve classified information.*
- *Using administrative powers to freeze or seize assets on the basis of confidential intelligence that could not be used to support prosecution.*

7. Argentina, Colombia, Chile, Panama, Paraguay, Peru and the Dominican Republic have signed the Budapest Convention on Cybercrime.

3.2. ADVANTAGES OF A PARALLEL FINANCIAL INVESTIGATION

109. Where resources are available, particularly the availability of financial investigators, there are great advantages to having a financial investigation in parallel with the criminal investigation. Clearly, all organized crime related offenses (terrorism, **WMD** proliferation, arms trafficking, drug trafficking, human trafficking, fraud, etc.) will generate the acquisition of cash and property and give rise to leads obtained through bank documentation and the physical movement of cash and criminal property that can lead to evidence useful to the investigation.

110. In practical terms, terrorism, **WMD** proliferation and **TF/PF** investigations are generally linked, although it is important to note that they need not be. To ensure that all relevant actors in the criminal network are uncovered, it is important to conduct systematic parallel financial investigations in each case involving terrorism or **WMD** proliferation. The investigation can be a stand-alone **FT/FP** investigation, or where appropriate, form part of a broader terrorism or **WMD** proliferation offense investigation. Many jurisdictions face challenges with investigative capacity to be able to conduct parallel financial investigations. Generally, financial investigations are not conducted if the underlying terrorist activity appears to be primarily self-funded or if the sums involved are very small.

111. Good practices include ensuring that a **TF/PF** investigation can be initiated without an underlying terrorism or **WMD** proliferation case, and that the **TF/PF** investigation can continue even when the linked terrorism or **WMD** proliferation investigation has already concluded. Another useful practice is to issue manuals and procedures for identifying and investigating **y**. In addition, financial investigations should be considered not only from a prosecution-oriented perspective, but also from an intelligence standpoint. .

112. The main advantages of parallel investigations in **FT/FP** cases are:

- *Identify the nexus between **LA, FT/FP** and organized crime.*
- *Identify the scope and structure of an organized criminal group, terrorist group, proliferation network, etc.*
- *Locate assets.*
- *Identify ownership and use of properties.*
- *Evidence of offenders' lifestyles that can be useful evidence of their involvement in crime.*
- *Tracking the movement of people and money*
- *Placing people in particular places at particular times, linking them to crime. Identify additional crimes and offenders.*
- *Identify additional crimes and offenders .*
- *Revealing undiscovered criminality .*
- *Helping to combat criminal networks by denying them the ability to fund more crime.*
- *Disclose links to **LA, TF/PF** and corruption.*
- *Obtaining evidence for confiscation.*

3.2.1. TEAMWORK

113. An investigation into **FT/FP** and the criminal networks on which such crimes are based benefits greatly from a team approach. The involvement of criminal investigators and financial investigators is obvious, but in addition experts such as accountants and computer technicians, other government employees such as customs officials, the **FIU**, the asset management department and tax inspectors may also be involved. The prosecutor will often be involved, depending on the position in the particular national jurisdiction, either advising or directing the course of the investigation.

114. In such a situation, it is understood that there are, in general terms, three basic requirements:

- *Legislation that allows "gateways" or a legal way for information to be shared between different departments and individuals.*
- *Interdepartmental memorandum of understanding **(MOU)** or service level agreements that detail how departments will relate to each other, e.g., how decisions will be made, how differences will be resolved, how each department will assign personnel to the team, etc.*
- *A strong personal and individual relationship between team members, based on mutual trust and respect.*

UNITED KINGDOM

An example of "gateways" in the UK is in the 2003 Courts and Crime Act , which provides a general procedure for the exchange of information involving the National Crime Agency (NCA); the 2001 Anti-Terrorism, Crime and Security Act which allows tax and customs departments to disclose information to assist in criminal investigations and prosecutions in the UK and overseas; and the 2017 Criminal Finances Act, which allows for the voluntary exchange of information between regulated sector agencies, and between those agencies and the NCA, in relation to suspected ML/TF activities.

115. Information sharing is often a challenge, as in some jurisdictions it is not unknown for information to be withheld rather than shared. It should be clear who will decide strategic issues in the course of the investigation and how differences will be resolved. As a matter of good practice, a strategy should be agreed at an early stage of an investigation and prosecution that includes the identification of team members, their respective roles, the need for any specialist advice, the need for **MLA**, the likelihood of restraint/freezing/confiscation of financial assets. Deadlines should be set for specific stages of the investigation and prosecution and regular meetings held to review progress and resolve any issues at an early stage. The strategy should remain flexible to take into account any developments, such as the emergence of new suspects and the identification of substantial new areas of investigation. An efficient information sharing system is essential to the success of **TF/PF** investigations.

116. An example of good practice is the research "working group" model. This may include setting up multi-disciplinary teams to conduct **FT/FP** investigations and collaborate on case development. Task forces may consist of a combination of specialized investigators from **LEAs** (such as counter-narcotics, tax, anti-corruption or customs agencies), prosecutors' offices, intelligence authorities and financial analysts. The exact composition of the task force depends on national practice, but the intent of the task force model is to leverage expertise, resources, tools and authorities in a joint investigative team to achieve the best results. Such models also help to avoid operational conflicts and group relevant authorities together, potentially with the effect of speeding up case completion and simplifying tasks. Another good practice is the creation of specialized **TF/PF** investigative units and prosecutorial designation. Task forces and special units should be adequately resourced, including staff with the necessary skills. Another good practice is to use special expertise such as forensic accountants, financial analysts and computer forensic experts in forensic investigations. If necessary, this expertise can be sought from sources outside the unit or task force.

3.3. GOOD PRACTICES IN FT/FP ANALYSIS AND RESEARCH

117. In **FT/FP** cases it is advisable to define a strategy in the analysis and investigation stage according to the following principles.

- *Identification of research objectives.*

118. Prioritization is key. The identification of targets, both natural and legal persons, will guide the preparation of the indictment at the end of the investigation. A standard form or model data sheet should be drafted and assigned to each of the identified targets. Each data sheet should contain details of surveillance carried out on the target, relevant conversations if communications have been intercepted, suspicious movements of bank accounts and any other information to support the indictment.

- *Participation of legal entities.*

119. The involvement of legal entities in **TF/PF** cases often poses challenges in identifying their "beneficial owners", i.e. the natural person who exercises control over the legal entities and their transactions. These challenges include:

- *Lack of accurate and updated beneficial ownership information because the companies did not update the corresponding information or did not inform the company's registry when there was a change in beneficial ownership.*
- *Difficulties in identifying beneficial ownership information when dealing with complex structures.*
- *Use of screen companies.*

120. Terrorist groups and proliferator networks often establish or use companies to hide the proceeds of their illicit activities. It is necessary to determine whether the companies are engaged in genuine business activity or whether they are merely "fronts". If they are engaged in a genuine business activity that, in turn, allows them to hide funds of illicit origin, it will be necessary to identify what proportion of the company's funds is illegitimate. To this end, for example, invoices, contracts and cash deposits in accounts with no discernible origin or accompanying documents justifying the transaction in question can be examined. Transfers between the companies of the person under investigation may also be identified as a way of concealing the true origin of the funds. Ultimately, expert reports will serve as a basis for identifying what proportion of the funds come from unexplained sources.

- *Asset tracking .*

121. At the same time as identifying the target, it is also necessary to identify the assets that can potentially derive from criminal activities, bank accounts, real estate and vehicles, etc. It is vitally important that all of the target's assets are clearly identified so that, if necessary, when the time comes to arrest the target, their accounts can also be blocked immediately.

- *Prioritize research objectives.*

122. It often happens that the investigation of a particular target leads to the identification of a new target, then another, and so on. If, in addition, there is a possibility that some of the as-

sets may be located abroad, which would require international cooperation, it is advisable to set a time limit for the investigation and prioritize the most important targets.

- *Circumstantial evidence*

123. When a target is arrested, it is very important to pay close attention to all documentation seized from the suspect during the search of his home or office, at the time of the arrest and in his vehicle, etc. This can reveal the target's relationship or dealings with other suspects, help identify assets or even prove that the target was aware of the illicit origin of the funds and/or their destination for terrorist or **WMD** proliferation purposes.

4. INVESTIGATIONS AND CONVICTIONS IN FT CASES

SPAIN

2022. Operation Kital

*Three people (two Libyan men and a Moroccan woman) were arrested in Barcelona, Girona and Valencia in February 2022 when they allegedly used a complex network of companies with an international presence to divert funds to a terrorist group linked to the Islamic State operating in Libya. The two Libyan nationals arrested were linked to the Libyan militias **Ansar al Sharia (ASL)** and the February 17 Martyrs Brigade, close to AQ and ISIL in Syria, Iraq and Libya. The investigation showed that the group had been active at least since 2014. The dismantled jihadist cell managed a criminal network of oil smuggling, fake passports, money in tax havens and the transfer of wounded terrorist fighters to private clinics in Barcelona and Madrid for healing. In addition, the group used human couriers, mostly Libyan students living in Barcelona, bank transfers and hawala structures to transfer money arriving in Spain from Libya undetected. The terrorist cell originated in Libya. The investigation focused on a group of fighters from Zawiya, a city near Tripoli. They were all members of the same **Islamic State (IS)** linked militia operating in the area, led by Mohamed Salem Bahroun, alias El Far (The Rat). This militia set up a base in Spain with two objectives. On the one hand, to finance the militia's activity, helping to channel out of Libya the money obtained irregularly, which came mainly from oil smuggling. On the other hand, the cell was in charge of receiving fighters linked to **IS**, wounded in the war, to treat them in private hospitals in Barcelona before returning to combat. Part of the money arriving from Libya left Spain to be transferred to Turkey or Tunisia and ended up in a tax haven, specifically in Antigua and Barbuda, where it was kept to be used when necessary. The dismantled cell even managed to obtain passports from these Caribbean islands to facilitate their movements and avoid detection in Spain and other European countries such as Germany. Another part of the money remained in Spain to cover the group's expenses.*

A Moroccan woman, also arrested during the operation, was in charge of paying for the medical insurance and specific treatment of the wounded terrorist fighters. The arrival of the patients was managed by the Libyan embassy in Spain. The cell chose the clinic, picked up the wounded and transferred them to the hospital. Once they were cured, they returned to fight. The head of the cell in Spain created companies in Badalona (Barcelona) to sell goods imported from Arab countries. However, the investigation revealed that this business had few clients and lacked sufficient real activity to justify its high level of income. Money movements of up to four million euros and one-off transfers of 600,000 euros, incompatible with the volume of the business, were detected. What was behind it, according to the investigations, was the thriving illegal oil trade carried out by the militia in Libya. The Spanish police are also investigating whether there was money laundering and illegal human trafficking. Money was moved from Spanish companies to fulfill their role with the militia led by Mohamed Salem Bahroun, alias El Far (The Rat). Some of the money was used to buy all-terrain vehicles used in combat. Some members of the jihadist militia were detected with these cars in combat training camps through Facebook accounts.

2019 - 2021. Operation Wamor

In 2019, the National Police launched the so-called 'Operation Wamor', one of the largest police operations against terrorist financing carried out in Spain. As a result of the investigations, ten people were arrested in Madrid, Valencia and Toledo, who were involved in sending money to Iraq and Syria. Of these, nine were Spanish nationals and one was Syrian. This cell, with its epicenter in the capital, was dedicated to financing the return of foreign fighters who had fought in the aforementioned conflict zones during the peak years of ISIL. The epicenter of Operation Wamor revolves around Fares Kutayni and his family, Syrians who arrived in Spain in the 1980s after the first purges of the Hafez al-Asad regime. Kutayni developed his business of buying and selling heavy vehicles and real estate services between Madrid and Valencia until acquiring Spanish citizenship. Like many other terrorists, he carried out 'Taqiyya', a practice that consists of 'posing as an infidel' so as not to arouse suspicion. Alerts sounded in December 2017 when the investigative services discovered that his son, Human, had returned to Spain after serving time in Syria for collaborating in an Al-Qaeda attack. As a result, they began investigating the family's high economic status and the existence of frequent money transfers to their country of origin, specifically to the Al-Qaeda militia, Hal'y Tahir al-Sam, of the al-Nusra Front, whose leader turned out to be Fares' brother, Manaf Kutayni. The agents managed to unravel a clandestine financial system based on the falsification of invoices, concepts and records of different companies. The detainees would deduct money from each legal transaction by replacing the actual amount of the transaction on the invoice with a lower amount. The difference would end up in a "b-box" and sent, in small amounts and in different ways, to

*the Syrian region of Idlib, where some of the detainees had family ties with members of the Al-Qaeda militias that subsist there. The money was sent by members of the organization using different systems. From the use of "human couriers" who moved the money illegally circumventing money laundering regulations, to sending suitcases with hidden money, remittance machines and above all using the hawala, an unregulated money transfer system that employs a network of mediators who use their businesses to transfer the funds to the desired country in small amounts. In April 2018, the detainees managed to activate a goods transport route for their business on the Damascus- Hama- Idlb and Turkey route. A passage only practicable for those with direct contacts in the terrorist militias that controlled the area and who put the necessary means for the effects of the detainees and the people they determined to reach the destination. Through cash remittances to avoid arousing suspicion, they managed to expand their links with Al-Qaeda far beyond Syria, reaching affiliates in Sudan, Yemen, Somalia and Libya. Through the legal cover of their company, they managed to send 'human couriers' to the area, via routes 'bought' from various militias. Once the foreign fighters' were in Spain, they were provided with accommodation in the Corredor del Henares area of Madrid. Four years after the beginning of this anti-terrorist operation, other sources of jihadist financing have come to light. The first of the three accused, Ayman Adlbi, president of the Islamic Commission in Spain, accused of financing terrorism, is currently at liberty awaiting trial. On the other hand, the treasurer of the Union of Islamic Communities of Spain (**UCIDE**), an organization located in the Islamic Center Abu Bakr Mosque in Madrid, has been remanded in custody without bail on charges of belonging to a terrorist organization and financing terrorism. The money transfers were made under alleged donations to an **NGO** for orphaned children in Syria, Al-Bashaer Humanitarian Organisation, linked to the jihadist organization Yeish al-Islam, an Al-Qaeda affiliate. These funds were intended for the training of mujahideen. The former president of the institution, Riay Tatary, made these donations during the course of his mandate until his death by Covid-19 in May 2021. They were charged with collaboration with a terrorist organization, membership of a criminal organization, terrorist financing, money laundering, forgery of documents, tax fraud and promotion of illegal immigration.*

2016. The tailors of ISIS

In March 2016 the police seized a container in the port of Algeciras (Cadiz) and two more in the port of Valencia. The first contained second-hand clothing, as had been declared to customs, but in the last two there was a packing machine and, hidden under piles of used clothing, five tons of bundles, perfectly packaged and marked, with some 20,000 unused military uniforms: enough to equip an entire army. The shipments were made by ship to Turkey and then by road to Syria. The company Tigre Negro S.L., a textile export company, was the cover. The container had arrived from Saudi Arabia - although the uniforms appear to have come from a NATO country - and was ready to be shipped to Turkey: first to the port of Mersin, off Cyprus; and then, by road, to the town of Bad al Hawa, on the other side of the Syrian border. The alleged ringleader of the plot was Ammar Termanini, born in Aleppo (Syria) in 1972, and landed in Spain in 2012, after having lived in Holland, Belgium and the United Kingdom. In Spain, he set up a company, Tigre Negro S.L., of which he was the sole administrator, dedicated to the export and import of textile products. Under the cover of bringing humanitarian aid, he made several shipments to Syria, where he traveled frequently.

The financier of Termanini's operations was Mohamed Abu El Rub Karima, born in Jordan in 1960 and a resident of Ontinyent. Uniforms like the ones later seized in the Valencia container were found in his warehouse in the L'Altet industrial park. To collect funds and make payments, he used hawala, the traditional Muslim system based on trust that allows money to be moved between different countries without leaving the trace of bank transfers. The ideologist of the group was allegedly Nourdine Chikar Allal, a Moroccan businessman living in Muro d'Alcoi and president of the Cocentaina mosque, who, thanks to his contacts in Turkey, was in charge of clearing the obstacles encountered by the shipments until they reached their final destination. The network not only sent uniforms to the Islamic State, but also handled any kind of order. For example, a type of fertilizer that is not sold in Spain and is used to produce explosives that Termanini would have ordered Hitham to purchase.

2018. TF through trafficking of antiques

In March 2018, the National Police arrested two Spaniards in Barcelona during an operation against the plundering of works of art in Libya, the sales of which made it possible to finance terrorism. The detainees were part of an international organization based in Catalonia, one of them being a renowned antiquities expert who had participated in various academic debates. This was the first operation to be carried out against this form of financing international terrorism through the illegal trafficking of works of art and antiques. Although the network was active in several countries, it was based in Catalonia. The organization owned in Barcelona and in the town of Argentina a workshop to restore the pieces, a warehouse where they were stored and the art gallery where they were exhibited for sale to the public. Because the pieces were extracted with violence and without using proper archaeological techniques, the detainees repaired them to erase the imperfections and the blows they suffered. Since the end of 2014, the main detainee and expert in ancient art had woven a network of suppliers around the world that allowed him access to archaeological pieces from various civilizations. In October 2016, he committed a series of irregularities in the import files of works he had acquired earlier, which caught the attention of investigators. The detainees used intermediaries abroad to search for the pieces and make them difficult to trace. They then bought them on behalf of the detainees and sent them from third countries to avoid attracting the attention of the Spanish authorities. On other occasions, they passed them off as decorative objects of no value and at a price much lower than the real price.

2018. FP Research

In 2018, an FI submitted a SAR to SEPBLAC regarding an attempted transaction from a foreign bank located in a Middle Eastern country to a Spanish company's account opened in a Spanish bank. This transaction was rejected by the Spanish bank as it was related to the purchase of industrial equipment on behalf of a third party located in Iran and the Spanish company could not properly justify it. Following the analysis of the attempted transaction and the underlying documentation, SEPBLAC identified that the Spanish company was specialized in the production of high-tech industrial equipment. SEPBLAC also compared the companies involved with the UN sanctions list and commercial databases and identified that the Iranian company had some links to the government of Iran. SEPBLAC shared this case with the National Police, the Civil Guard and several Spanish intelligence services for further investigation.

2018. FP Research

In 2018, one of the Spanish intelligence agencies informed SEPBLAC about a Spanish national who might be involved in evading UN sanctions related to the DPRK, in particular established under UNSCR 2397. SEPBLAC was able to identify several bank accounts opened by this Spaniard in Spanish banks and one bank account opened in another European country. No matches were found with the UN sanctions list during the analysis; however, SEPBLAC discovered that the Spanish national had previously been under police investigation. SEPBLAC also cooperated with its FIU counterparts through FIU.NET and identified that some low-value transfers were routed through this national's foreign account, while the domestic accounts were not in use. The results of SEPBLAC's operational analysis were shared with the National Police and the Guardia Civil, who continue to investigate this case.

December 2018. FT Research

As a result of investigations by the National Police's General Information Office, four Syrian nationals were arrested in as many Spanish prisons for having participated, while at liberty, in various TF activities providing economic support to terrorist groups operating in the Horn of Africa and Syria. Investigations have revealed that the network transported drugs through Mediterranean waters, mainly to Libya, with the aim of financing insurgent groups in the area. In that North African country, they exchanged the drugs for weapons, which were then destined for terrorist groups in conflict zones. These boats were also used to traffic immigrants from Syria and Libya to the coasts of Europe, mainly Greece, Italy, Cyprus and Malta. This illegal human trafficking has also served to finance terrorist activities.

2012. Operation KAMPAI

A cell that provided documents to the Al-Qaeda terrorist network was dismantled in late 2012 and early 2013, leading to the arrest of eight people belonging to a cell linked to Al-Qaeda, which provided Al-Qaeda and other terrorist organizations with travel documents (mainly passports) stolen in Spain and then sent to Thailand, where they were forged for delivery to terrorist and organized crime groups, allowing them to cross European borders and other Western countries.

2011. Operation NOVA

In connection with the investigation of the terrorist organization Mártires por Marruecos, which was planning attacks against the Supreme Court, Audiencia Nacional, and other institutions in our country, a terrorist organization directed from inside the prisons was dismantled, where they recruited members for their cause dedicated to crimes against property and hashish trafficking (Ruling SAN 8/11).

2009. Operation TIGRIS

(Disarticulation of a cell linked to international terrorism that provided support and coverage to Al-Qaeda terrorists), in sentence no. 31/2009 of April 30, 2009, issued by the Audiencia Nacional, whereby the members of said cell were prosecuted, it is stated that, although neither the ownership of the merchandise nor the drug trafficking has been proven, how one of the defendants had 808 grams of hashish and a precision scale used for the distribution of the drug seized in his home.

2006. Operation CESPED

Two persons were convicted of terrorist financing activities, by means of money transfers (through a call shop in Logroño, whose manager performed the functions of Hawaladar), transfers, checks, checks charged to bank accounts and promissory notes, following instructions from a well-known Al-Qaeda militant, which culminated in the attack on the La Ghriba synagogue on the island of Djerba in Tunisia, on 11-04-02. Ruling nº 20/2006 of May 9, 2006 by the Audiencia Nacional and ratified by the Supreme Court.

2005. Operation GAMO

In November 2005, the investigation led to the detection and location in the cities of Alicante and Granada of an alleged "logistical cell" dedicated to the financing and logistical support of the activities of the former Algerian Salafist Group for Preaching and Combat (GSPC). The activity of the cell was focused on various common criminal activities covering a wide spectrum: document forgery, drug trafficking, credit/debit card forgery, theft of property and vehicles, receiving, possession of forgery tools and forgery of official documents. The investigation was the subject of proceedings initiated by the Juzgado Central de Instrucción nº4.

2005. Operation QUEIXALADA

In Barcelona in 2005, ten individuals of Pakistani origin were arrested on suspicion of belonging to a Pakistani cell in Spain responsible for the financing and logistical support of the Islamist group Sunni Tehrik, considered terrorist by the Pakistani authorities, being reflected in the judgment number 39/2007 of May 28, of the Audiencia Nacional, and also ratified by the Supreme Court, the conviction for collaboration with a terrorist organization, of a Pakistani terrorist cell based in Barcelona. For this purpose they formed a perfectly organized group, being charged with other crimes such as document forgery, currency counterfeiting and drug trafficking.

2004. Operation GREEN

The facts investigated and subsequently ratified by the judgment of the National Court No. 17/2010 initiated by a series of robberies in the southern area of Spain in 2004, allegedly committed by a cell dedicated to obtaining economic resources for the financing of international terrorist groups (Salafist Group for Preaching and Combat, currently Al-Qaeda in the Islamic Maghreb-AQMI), by which the public prosecution maintained the existence of a criminal group or organization whose main activity would be dedicated to the financing of the Salafist Group through the commission of robberies in an organized manner in luxury homes along the Andalusian coast, stealing jewelry, money, credit cards and cell phones and their subsequent marketing by some members of the organization, thereby obtaining amounts of money for its financing. Even one of them, who acted as hawaladar in Algeria, who traveled frequently to Spain and had a relationship with the accused, was convicted by a Criminal Court of Oran, for a crime of belonging to a terrorist organization acting abroad, facts committed in 2005 in a foreign country, by virtue of the official complaint filed by the Spanish authorities before the judicial authorities of Algeria.

Convictions FT (International Terrorism)

- Creation of an international network of companies to finance the Islamic State and contribute to the development of drones (Judgment of April 27, 2020 of the Audiencia Nacional).

- Raising funds for a terrorist organization (Al Ansar, linked to Al-Qaeda) by collecting alms (Judgment no. 5304/2011 of the Audiencia Nacional).

- Financing travel expenses and providing material support (such as accommodation) to an Islamist terrorist movement (Judgment no. 1943/2011 of the Audiencia Nacional, which was also a case of self-financing).

- Mobilizing funds through a "hawaladar" to Algeria on behalf of Islamist terrorist groups. The defendants were members of a group dedicated to obtaining financial resources for a terrorist group in Algeria. The funds were sent from Spain through a hawaladar (Judgment No. 2591/2010 of the Audiencia Nacional) and through money transfer companies, as well as the transport of cash by courier to various countries in North Africa (Judgment No. 1943/2011 of the Audiencia Nacional).

- Mobilizing funds to commit a terrorist attack (car bombing of a synagogue on the island of Djerba in Tunisia) (Judgment no. 6284/2006 of the Audiencia Nacional). The trial led to the conviction of two businessmen for having transferred money to the family of the suicide driver of the tanker truck used in the attack and to recognized members of Al-Qaeda. This case is important because the conviction imposed by the Audiencia Nacional was based on circumstantial evidence, as well as on the assessment, in particular, of links and contacts with persons in the orbit of Al-Qaeda, the transfers and delivery of money on the instructions of and for the benefit of these persons, the absence of any lawful business activity to justify these operations and the concealment of the supporting documentation for these movements and transfers.

- Using funds to help terrorists who fled after committing the 11-M train bombings in Madrid (Judgment No. 1943/2011 of the Audiencia Nacional). The defendants financed the escape of some of the terrorists who had participated in the 2004 attacks in Madrid. The terrorist financing activity consisted of providing them with accommodation and financing their travel expenses. The defendants were convicted of the crime of membership in a terrorist organization. The court confirmed that membership "implies the provision of some kind of service for the achievement of the group's objectives in the ideological, economic or logistical field, or in the execution of the objectives".

Convictions FT (ETA)

- Raising funds for a terrorist organization (ETA). The accused was a member of ETA and was in charge of the operation of the organization's economic network, including the collection of donations and donations through taverns known as txoznas (Judgment No. 39/2008 of the National Court), raffles (Judgment No. 4382/2010 of the National Court, for attempted financing of terrorism), and by conducting an extortion campaign to collect the so-called "revolutionary tax" (Judgment No. 3108/2011 of the National Court).

Coordinating and managing a business group responsible for financing a terrorist organization (ETA) through a complex web of large companies and profitable businesses, including a travel agency, an event supply rental company, a financial management company and an insurance company (Judgment No. 73/2007 of the National Court). The defendants ran ETA's economic apparatus, made up of a network of large and small companies and profitable businesses, whose profits were channeled to the organization to finance its political and terrorist activities. Among their functions were the incorporation and management of companies and the financing of ETA's activities.

FRANCE: FT research through cryptocurrencies

In September 2020, French police arrested a terrorist financing network using cryptocurrency vouchers in licensed tobacco stores across France. Since 2019, the detainees were supporting the operations of an Al-Qaeda affiliated terrorist organization called Hayat Tahrir Al-Sham. The 29 members of the network were arrested after being caught buying cryptocurrency coupons worth between €10 and €150 each (USD 12 - USD 176) on multiple occasions at different tobacco outlets in France. These outlets, known in French as tabacs, were integrated into crypto coupon services in 2019 to encourage the adoption of cryptocurrencies by the French public. Suspected terrorists would purchase these cryptocurrency coupons in France, scan and send the images to the group's leaders, two French nationals residing in Syria. The coupons were then converted into Bitcoin via Turkey. Although customers have to provide their IDs to register an account on the coupon issuers' websites and receive their Bitcoin, the terrorist group's leaders successfully managed to activate their Bitcoin codes. They did so despite having been sentenced in absentia to 10 years in prison and international arrest warrants had been issued against them. A cryptocurrency token is a ticket that includes a numeric code, or a two-dimensional barcode, to pass the purchased cryptocurrency to a digital wallet. Wallet providers must screen customers for anti-money laundering purposes when they onboard them, but the purchase of coupons does not automatically trigger due diligence processes in and of itself. In addition to the coupons that the defen-

dants used to credit the Bitcoin accounts of their Syrian accomplices, these tabacs support a range of small payment services, such as cash card top-ups and cash coupons. These services, in particular, do not require proof of identity. The case demonstrates that cryptocurrency tokens can protect transaction originators from identification. But the beneficiaries of those transactions still run the risk of being detected the moment they try to convert the coupons into government-issued bills on a cryptocurrency exchange.

UNITED KINGDOM

In June 2019, the parents of a British citizen who traveled to Syria to join Islamic State were convicted of FT after the prosecution found their son to be part of a terrorist organization and it was deemed proven that they sent £223 (€250) in September 2015 to their son, Jack Letts, a Muslim convert renamed by the media as 'Jack the Jihadist'. Letts left his Oxford home at the age of 18 to travel to Jordan and Kuwait, allegedly for educational and tourism reasons. As early as March 2015, British police warned his parents that they risked prosecution if they sent him money, but in September his mother paid money into a bank account in Lebanon after her son assured her that he had "nothing to do with jihad."

COLOMBIA

August 29, 2014

Sentence issued by the Seventh Criminal Court of the Specialized Circuit of Bogotá (29-08/2014). The defendants were engaged in activities of commercialization of firearms and other related elements of restricted use, destined to the FARC armed group. They were convicted for the crime contemplated in Article 345 of Law 599 of 2000 (Criminal Code) financing of terrorism and organized crime groups and administration of resources related to terrorist activities and organized crime, for the conducts of promoting, supporting and maintaining.

August 21, 2013

Criminal Court 1 of the Specialized Circuit of Bogota. Supplies (uniforms, harnesses, vests, rifle racks, telescopic sights, backpacks, field boots, hammocks, blankets, communication radios, night vision goggles), weapons, ammunition and explosives. FARC. Judgment of August 21, 2013 issued within the process with C.U.I. 110016000027201000055 advanced by the First Criminal Court of the Specialized Circuit of Bogota. Six defendants were convicted for the crimes of: (i) Aggravated Conspiracy to commit a crime (Art. 340 Criminal Code), (ii) Financing of Terrorism and Organized Crime Groups and Administration of Resources Related to Terrorist Activities and Organized Crime (Art. 345 Criminal Code), as well as (iii) Manufacture, trafficking and carrying of weapons, restricted use ammunition, ammunition for the private use of the Armed Forces or Explosives (Art. 366 Criminal Code). The facts are related to the supply of supplies and weapons to the illegal armed group FARC.

November 5, 2010

Criminal Court 1 of the Specialized Circuit of Cúcuta. Support from the security cooperative to the ÁGUILAS NEGRAS organization through money, white identification, vehicles, human resources. Ruling of November 5, 2010 issued within the action 54-001-31-07-001-2009-00063-01 whose first instance corresponded to the First Criminal Court of the Specialized Circuit of Cúcuta and the second confirmatory to the Criminal Chamber of the Superior Court of Cúcuta. In this case seven defendants were convicted for the crimes of: (i) Financing of Terrorism and Organized Crime Groups and Administration of Resources Related to Terrorist Activities and Organized Crime (Art. 345 Criminal Code), as well as (ii) Aggravated Homicide for Terrorist Purposes (Arts. 103, 104.8 Criminal Code). The facts have to do with the support provided by the Security Cooperative COOTRAVI to the criminal organization Águilas Negras, not only with money, but also with human resources (security guards of the cooperative), transportation of weapons and identification of targets.

August 25, 2010

Criminal Court 2 of the Specialized Circuit of Cúcuta. Provision of food and other items such as mattresses for the group AGUILAS NEGRAS. Sentence issued by the Second Criminal Court of the Specialized Circuit of Cúcuta (25-08/2010), fully confirmed by the Criminal Chamber of the Superior Court of Cúcuta. Two defendants were convicted for the crime of financing terrorism and organized crime groups and administration of resources related to terrorist activities and organized crime (Art. 345 Penal Code). The facts took place in the Municipality of Ocaña where the criminal organization Águilas Negras operated. One of the convicted persons was the commander of one of the factions of the group, and the other was in charge of providing food and other elements such as mattresses to its members.

2008 -2009 Provision of arms to FARC

During 2009 and 2010 an individual was engaged in selling weapons to the FARC front. Upon execution of a search warrant issued on the basis of information obtained mainly through legal wiretaps, the police found illegal weapons. Subsequently, it was shown that this material was destined for the FARC. The court considered that FARC is a group that executes terrorist acts; also, that the supply of arms to FARC represents the provision of assets and support to an organization that commits terrorist acts. Therefore, that providing arms to FARC constitutes TF. The UIAF through its reports collaborated to prove that the buyers were FARC members and to establish the relationship of the defendant with those members through the analysis of the financial operations. In addition to the sanctions for arms trafficking, since the individual was not a member of the FARC, he was sentenced to 13 years in prison for a TF offense.

July 13, 2007

Criminal Court 2 of the Specialized Circuit of Ibagué. Collection of money through extortion for an irregular group called "Nueva Generación de las Autodefensas del Bloque Tolima" (New Generation of the Self-Defense Forces of the Tolima Block). Sentence issued by the Second Criminal Court of the Specialized Circuit of Ibagué (July 13, 2007), subsequently confirmed by the Criminal Chamber of the Superior Court of Ibagué. The facts that originated the judicial pronouncement are related to the extortion activities that the defendants carried out in the Department of Tolima on behalf of the irregular armed group "Nueva Generación de las Autodefensas del Bloque Tolima" (New Generation of the Self-Defense Forces of the Tolima Block). Under this modality they were in charge of sustaining the finances of said group, being finally convicted for the crime of financing terrorism and organized crime groups and administration of resources related to terrorist activities and organized crime (Art. 345 Penal Code). In this case it should be noted that in addition to this sentence, they were previously convicted for the typology itself, i.e. the crime of extortion.

CHAPTER III

STRATEGIC PROCEDURES WITHIN THE FRAMEWORK OF INTERNATIONAL COOPERATION FOR THE PREVENTION, DETECTION, INVESTIGATION AND DISRUPTION OF FT/FP.

1. INTRODUCTION

124. The collection of financial intelligence to detect financial networks linked to terrorist groups and or linked to **WMD** proliferation, including information sharing between **LEAs** and regulatory agencies, is an essential part of all strategic approaches to combating terrorism and WMD proliferation.

125. The international community has acted on many fronts to respond to the increasing complexity and rapid evolution of new typologies of **TF/PF** and to establish a coordinated and effective international regime to combat **CTF/CPF.** The specific obligations of countries in relation to this regime vary depending on their adherence to the various treaties. Within this global regime, due to the relative ease with which funds intended for terrorist or **WMD** proliferation purposes can move internationally, countries with weak mechanisms for combating **TF/TFPs** are particularly vulnerable to these criminal activities.

126. Successful investigation and prosecution of **TF/PF** requires the rapid identification of relevant information from banks, other financial and non-financial institutions and commercial businesses. Asset tracing and confiscation, both within a jurisdiction and internationally, are hampered by the complexity of banking systems and financial institutions. Technological advances hinder these efforts. The fact that many transactions are transnational requires changes in bilateral treaties and national legal frameworks to allow for the legal and rapid exchange of such information between **LEAs** in different countries. In this regard, the existence of unregulated offshore centers presents additional practical problems from the point of view of international cooperation between **LEAs** due to the difficulties that often arise from differences in corporate law and other applicable regulatory standards. Likewise, cyber payments and the existence of "virtual banks" operating in under-regulated offshore jurisdictions and shell companies operating outside the territory of offshore centers also pose significant challenges.

2. STRATEGIC PROCEDURES IN THE FRAMEWORK OF INTERNATIONAL COOPERATION CTF/CFP

127. In the context of the global fight against **TF/PF,** timely information exchanges and effective international cooperation between the various agencies in different countries have become a prerequisite in the financial intelligence gathering and analysis, investigation and prosecution stages of successful prevention and disruption of these criminal activities. The ability to rapidly exchange information with foreign counterparts, without undue hindrance or delay, is increasingly becoming a key aspect of the work of **FIUs** and **LEAs**.

128. Moreover, considering that terrorist groups and proliferator networks are always seeking safe havens in countries with lax, ineffective, corrupt **AML** and **CTF/CPF** regimes and limited information-sharing capabilities, having an adequate international cooperation framework in place allows States to prevent, detect and prosecute **TF/PF** in their own national jurisdiction.

129. In order for countries to use the existing channels of international cooperation, they need to meet several prerequisites, including the following:

- *Develop a broad and effective national capacity.*
- *Ratify and implement international conventions and **UNSCR** with respect to **LA** and **FT/FP**.*
- *Comply with the recommendations of the **Financial Action Task Force (FATF)** as well as with other international standards specific to each sector.*

130. A prerequisite for a country to be in a position to cooperate internationally with its partners is to develop a comprehensive and effective national capacity, establish the necessary bodies and provide them with the required powers, responsibilities, staff and budget, so that they can carry out their functions effectively. Among other things, in order to have an effective **anti-TF/PFT** framework, a country should have established other administrative and supervisory bodies to monitor institutions in each sector, as well as an **FIU,** i.e., a central authority in charge of receiving and analyzing suspicious transaction activity information and other types of mandatory reporting (such as cash transaction reports), in order to combat **ML** and **TF/PFT.** Likewise, in terms of the criminal justice system, countries should have effective police services with specialized knowledge and training in **FT/FP** investigations, as well as a criminal justice system with specialized judges and prosecutors in these matters. Adequate development of these entities, as well as the allocation of appropriate personnel, provides a basis for building a comprehensive and effective legal framework to combat **ML, TF** and **FP**, both domestically and internationally.

131. All countries must sign and ratify the relevant conventions adopted by the **United Nations (UN) .**[8] In addition, countries should sign and ratify the other conventions adopted by other organizations in their respective regions. [9]Countries must fully incorporate all the provisions of these international instruments into their national legislation, including those related to the criminalization of **FT.** This will enable them to participate in the **MLA** agreements stipulated by these conventions and facilitate extradition processes.

132. Countries must comply with existing international standards for combating transnational organized crime, **ML** and **FT/FP**. These standards include the **FATF recommendations,** the Core Principles for Banking Supervision, adopted by the Basel Committee on Banking Supervision (the Basel Committee), and its Customer Due Diligence Principles and the standards of the **International Association of Insurance Supervisors (IAIS)** and the **International Organization of Securities Commissions (IOSCO)** and the Egmont Group. Each of these bodies requires each state to maintain international channels of cooperation with third countries. For example, the **FATF in its Recommendation 30** states that "each country should make efforts to increase the spontaneous (or on request) exchange of information relating to suspicious transactions, persons or companies involved in such transactions, between competent authorities". In addition to the general principles on international cooperation, there are specific conditions that apply to international cooperation between **FIUs** and financial supervisory authorities, as well as between **FIUs** and **LEAs**, e.g. those contained in **FATF Recommendation 40** on other forms of international cooperation.

133. According to relevant international standards, countries should apply the following general principles to ensure that effective avenues for information exchange and international cooperation are in place at each stage of a **TF/PF** investigation:

- *When an authority in country A has information that has been officially requested by another authority in country B, the authority in country A, from whom the information is requested, should be in a position to promptly provide such information to the requesting authority in country B.*

8. In particular, countries should sign and ratify the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988) (Vienna Convention), the United Nations Convention for the Suppression of the Financing of Terrorism (1999), the United Nations Convention against Transnational Organized Crime (2000) (Palermo Convention) and the United Nations Convention against Corruption (2003).

9. Convention on Laundering, Search, Seizure and Confiscation of the Proceeds of Crime (1990) (Strasbourg Convention) and the Inter-American Convention against Terrorism (ICAT) within the framework of the Organization of American States (OAS).

- *When an authority in country A has information that it knows will be useful to an authority in country B, the authority in country A should be able to provide such information spontaneously and promptly to the authority in country B.*

- *When an authority of country B requests an authority of country A to obtain information or a document, or to conduct an investigation or inquiry, or to carry out a specific action, which will be useful in the context of an analysis, investigation or prosecution against the **TF/PF**, the authority of country A, from whom the information is requested, should be in a position to carry out the requested action (of course, if this action is permitted by the standards governing the performance of its functions at the national level).*

134. This exchange of information with a foreign authority, as well as the provision of assistance and cooperation to it, should not be subject to unduly restrictive conditions. However, it is generally accepted that the requested authority may subject its assistance to certain conditions. For example, the requested authority may subject its assistance to the following principles and stipulate that the requesting authority:

- *Performs functions similar to those of the authority from whom the information is requested (principle of specialty).*

- *Describe in your request the purpose or scope of the information to be used, and such information, once transmitted by the requested authority, should be treated by the requesting authority according to the scope of your request (transparency principle).*

- *Is subject to confidentiality provisions similar to those applicable to the authority from whom the information is requested (confidentiality principle).*

- *Is itself in a position to exchange information with the authority from which the information has been requested (reciprocity principle).*

135. International cooperation must be present at the different stages of a **TF/PF** investigation:

- ***Step 1:** Compliance with prevention and detection requirements*

136. The cross-border nature of financial flows and the development of business conglomerates with large international networks make it increasingly necessary for supervisors and regulators to adopt an international approach when assessing the implementation of **AML** and **CFT/CPF** obligations. This is a prevailing trend in banking sector supervision, where supervisors are working to increase their coordination and cooperation in the supervision of banks operating in multiple countries. A risk-based approach to institutions internationally exposed to being used by money launderers and/or terrorist financiers and/or **WMD** proliferation financiers is a key tool to enhance international coordination and cooperation among supervisors.

- ***Step 2:** Gathering financial intelligence*

137. The cross-border nature of financial flows and the development of business conglomerates with large international networks make it increasingly necessary for supervisors and regulators to adopt an international approach when assessing the implementation of **AML** and **CFT/CPF** obligations. This is a prevailing trend in banking sector supervision, where supervisors are working to increase their coordination and cooperation in the supervision of banks operating in multiple countries. A risk-based approach to institutions internationally exposed to being used by money launderers and/or terrorist financiers and/or **WMD** proliferation financiers is a key tool to enhance international coordination and cooperation among supervisors.

- ***Step 3:** Research*

138. The same can be said of the investigation stage by **LEAs** in **TF/PF** cases. The rapid exchange of information with their foreign counterparts, without hindrance or undue delay, is increasingly becoming a key feature of any investigation conducted by **LEAs.** Moreover, considering that money launderers, terrorist financiers and **WMD** proliferation financiers are always seeking safe havens in countries with lax, ineffective and/or corrupt **AML** mechanisms and **CTF/CPF** regimes with limited capacities for international cooperation. In addition, having an adequate international cooperation framework in place helps countries to prevent, detect and prosecute **ML** and **TF/CFP** in their own national jurisdiction. Several international bodies, and in particular Interpol, encourage international cooperation at the investigative stage in **ML** and **TF/TF/PF** cases.

- ***Stage 4: Processing***

139. **MLA** is a fundamental tool for **AML/CFT** prosecution associated with specific and formalized forms of international cooperation to ensure the procedural admissibility of evidence obtained abroad. Experience has shown that these objectives can and should be reconciled, provided that, first, the specificities of **MLA** are recognized; second, they are not abused to undermine international cooperation, in particular by imposing undue restrictions; and, finally, that countries are clear about the requirements and conditions for

MLA. FATF Recommendations 36 and 37 emphasize the importance of MLA and FATF Recommendation 40 encourages countries to provide the widest possible range of international cooperation. A detailed analysis of **MLA** processes and their application in the investigation and prosecution of **TF/PF** cases is provided in section 2.2. of this chapter.

2.1. JOINT TRANSNATIONAL RESEARCH TEAMS

140. In complex and time-sensitive cross-border investigations, speed and efficiency are critical. However, in many cases, traditional **MLA** channels do not fully meet the operational needs of the authorities involved. Cooperation and direct communication between authorities is the most effective method of handling the increasing sophistication of criminal activities of organized crime, terrorist groups and proliferator networks. **Joint investigation teams (JITs)** offer national authorities in different states a flexible framework that is relatively quick and easy to establish and allows the respective authorities to participate in the investigation in a mutually beneficial manner. Once a **JIT** has been established, partners can exchange information and evidence directly, cooperate in real time and conduct operations jointly. In addition, **JITs** allow professionals to be present during investigative measures in each other's territories and thus share their technical expertise and human resources more efficiently. Direct contacts and permanent communication allow **JIT** members to build personal relationships and trust, leading to faster and more efficient cooperation.

141. A **JIT** is an international team formed by mutual agreement by the competent authorities of at least two countries for the purpose of investigating a criminal case with transnational elements. The States participating in the establishment of a **JIT** decide on its composition, purpose and duration. The competent authorities of one or more countries may decide to establish a **JIT** for a specific purpose and for a limited period, which may be extended by mutual agreement. A **JIT** may consist of **LEA** officers and other relevant personnel. The **JIT** is headed by a member from the country in which it is based. And it is the law of that country that governs the **JIT's** activities.

142. **JITs** do not replace or change national legislation, nor do they replace international cooperation mechanisms through letters rogatory. However, an **ITC** is a robust and effective tool that enables cooperation when:

- *A domestic criminal prosecution requires a difficult and demanding investigation involving connections with third countries.*
- *Several countries are investigating criminal offenses where the nature of the case requires coordinated and concerted action in the States involved.*

143. An **ECI** allows its members:

- *Share information directly with each other without the need to resort to numerous mutual legal assistance requests.*
- *Requesting investigative measures between team members directly, dispensing with the need for mutual legal assistance requests. This also applies to requests for coercive measures.*
- *Be present at house searches and interviews within all jurisdictions involved, helping to overcome language barriers.*
- *Coordinate efforts in the field and informally exchange expertise.*
- *Build mutual trust between professionals from different jurisdictions working together and decide on investigative and prosecutorial strategies.*
- *Secure potentially available funding.*

144. International standards have recognized the value of forming joint investigation teams **(JITs)** for the purposes of cross-border investigations. This is particularly useful when an offense involves multiple jurisdictions. The **FATF** Interpretative Note to **Recommendation 40** on international cooperation suggests that law enforcement authorities should be able to form joint investigative teams to carry out cooperative activities in the course of their **TF/PF** investigations. Until recently, joint investigation teams were generally formed only in crimes related to transnational organized crime. The financial aspect of an investigation was often forgotten or not included in **JIT** agreements. This is beginning to change and **GAFILAT** jurisdictions would benefit from joining this emerging trend by ensuring that the financial investigation linked to **FT/FP** is included in any **JIT** agreement.

145. There is no rule on when to set up an **ECI** or when to use traditional methods of international cooperation between countries. Once an **JIT** agreement is in place, it is not necessary to continually send **MLA** requests between states for cooperation. The agreement provides a general legal basis for a range of consultations to be conducted, including financial consultations if so stipulated in the agreement, and creates a legal framework for national jurisdictions to work on a particular criminal case for a specific purpose. Therefore, **JITs** are often the best option for more serious and complex cases and investigations that require rapid and smooth coordination and the exchange of many files, documents and perhaps evidence over a longer period of time. It is not useful to use a **JIT** for a case that requires one or two investigative actions in another country over the course of a few weeks.

146. Due to their transnational nature, **JITs** have particular characteristics that differ from the characteristics of national research to facilitate the conduct of international research. These characteristics relate particularly to the assumptions of information sharing and data protection, evidence management and accessibility, as well as the way in which **JITs** are evaluated once completed, and how they are funded.

147. During the operational phase of an **JIT,** the exchange of information between members of different jurisdictions is carried out on the same basis as if all persons involved were within the same jurisdiction. Individuals from different jurisdictions share information with each other, which originates in their own countries. Traditional **MLA** requests do not need to be issued to receive information from an **ECI** member.

148. National law continues to play an important role in determining whether it is possible for a **JIT** member to provide the team with information from his or her own jurisdiction. A team member may only share information where it is possible to do so in accordance with the national law of his or her jurisdiction and within the established legal limits.

149. Best practices in relation to **ECI** training include:

- *The application of **UN** Conventions **(UNCAC, UNTOC)** or bilateral agreements as a common legal basis for the creation of a* **JIT.**
- *The participation of diplomatic channels in countries with which there is no cooperation.*
- *The involvement of central authorities in assessing whether it is appropriate to cooperate with third countries where the protection of human rights may be at stake. On this last point, it should be noted that there are also occasions when the involvement of central authorities may delay the creation of a **JIT.***

FRANCE, BELGIUM, NETHERLANDS

ML/FT network through hawala dismantled by transnational CBI

*In 2016 authorities in France, Belgium and the Netherlands dismantled an **LA/FT** network whose members operated in Western Europe and Morocco. The field action conducted with the support of Europol by more than 450 police officers simultaneously in France (Gendarmerie Nationale), Belgium (Police Judiciaire Fédérale) and the Netherlands (Nationale Politie) resulted in the arrest of 36 suspects. Members of the **JIT** had been investigating since 2015 the activities of this complex structure involved in **LA/FT** in Morocco through the proceeds of drug trafficking in Europe, with a total amount of funds already laundered estimated at over €300 million. The criminals' modus operandi involved the use of couriers who traveled by car and collected the proceeds of drug trafficking throughout Western Europe (collection rate of over €1 million per month) and transported them to Belgium and the Netherlands. The cash was laundered in Morocco through the Middle East using unregulated financial channels (the Hawala system), leaving no revealing evidence for investigators. Eurojust was asked to facilitate the transmission and execution of letters rogatory and to assist a **JIT** consisting of France, Belgium and the Netherlands. Europol supported this operation since July 2015 by providing analytical and operational support (cross-matching, operational analysis and business intelligence reports) to all countries involved. More than €5.5 million in cash was seized, in addition to gold worth €800,000, two semi-automatic weapons and ammunition. At all stages of this complex investigation, the exchange of information between national authorities, Europol and Eurojust was crucial.*

NIGER

ECI CT Niger: Joint Investigative Team in the fight against terrorism and its financing

*Since February 2021, this project, inspired by the ECI NIGER to fight against the irregular smuggling of migrants and human trafficking, aims to contribute to the fight against criminal networks linked to terrorism in Niger, through the creation of a joint investigation team **(JIT)** within the Central Service for the Fight against Terrorism and Organized Transnational Crime **(SCLCT/CTO).** The main lines of action of this project are to strengthen operational and judicial capacities, to improve the rate at which investigations are resolved and to support regional judicial and police cooperation between the services involved in the fight against terrorism, particularly in the Tillabéri area, known as the three border zone (Mali, Niger and Burkina Faso). The project led by France **(CIVIPOL)** and managed by the FIIAPP and the work of the Spanish National Police specialists to support the Nigerian police in the efficient operation of the criminal chain in counter-terrorism crimes.*

MERCOSUR

*On August 12, 2010, the Argentine Republic, the Federative Republic of Brazil, the Republic of Paraguay, the Oriental Republic of Uruguay (as **MERCOSUR** States Parties), the Plurinational State of Bolivia, the Republic of Ecuador and the Republic of Colombia (as **MERCOSUR** Associated States), decided to strengthen international cooperation in criminal matters and signed the "Framework Cooperation Agreement between the States Parties of*

MERCOSUR *and Associated States for the creation of Joint Investigation Teams", the purpose of which is to fight organized crime in all its forms* ***(MERCOSUR/CMC/DEC n.° 22/10).***

It is undeniable that the ***"Framework Cooperation Agreement between the States Parties of MERCOSUR and Associated States for the creation of Joint Investigation Teams"*** *has a highly significant value; In addition to the fact that its norms exhaustively regulate the formation and operation of the JITs, it is the first international instrument specially designed to be applied at the regional level among the* ***MERCOSUR*** *member states (to date) and open for signature (ratification and deposits) by the Associated States, which will allow the JITs to have a legal basis for their operation in twelve Latin American countries once all the States that make up the regional bloc have adhered to it.*

Joint Investigation Team, signed in June 2019 between the Prosecutor's Offices of Chile, Colombia and Ecuador, on Drug Trafficking and Drug Trafficking in Latin America and the Caribbean.

This tripartite agreement - signed on the basis of United Nations standards - the Public Prosecutor's Offices of the three States involved are both competent authorities and central authorities, which greatly facilitates communication when setting up the JIT (from the competent authorities, which are the bodies with legal capacity for criminal investigations) through the established legal channels (the central authorities, which in turn are the Public Prosecutor's Offices). All this facilitates cooperation and direct communication between competent authorities in criminal investigation and prosecution, justifiably involved in the complex criminal cases that lead to the formation of JITs.

Joint Investigation Team (Agreement for constitution), signed in the month of July 2019 between the Prosecutor's Office of Paraguay and the Ministry of Justice and Public Security of Brazil, in matters of human trafficking, drug trafficking and others.

Operational and creation instrument of the JIT, signed in August 2019 between the Prosecutor's Offices of Paraguay and Brazil. This bipartite agreement, signed based on United Nations standards, required a prior framework agreement between central authorities (Prosecutor's Office for Paraguay, Ministry of Justice for Brazil) to authorize the creation of the JIT and, subsequently, the JIT itself was signed between Competent Authorities (Prosecutor's Office for Paraguay, Attorney General's Office - Prosecutor's Office - for Brazil).

Joint Investigation Team (Agreement for constitution), signed in the month of July 2019 between the Prosecutor's Office of Paraguay and the Ministry of Justice and Public Security of Brazil, on organized crime, arms trafficking, drug trafficking and others.

Operational and creation instrument of the JIT, signed in August 2019 between the Prosecutor's Offices of Paraguay and Brazil. In this bipartite Agreement, there were the same variables explained above.

Joint Investigation Team, signed in August 2020 between the Prosecutor's Offices of Chile and Peru, in the area of Smuggling of Migrants.

In this bipartite agreement - signed on the basis of United Nations standards - the same variables explained above were present.

Joint Investigation Team, signed in September 2020 between the Prosecutors' Offices of Argentina and Uruguay, in matters of Drug Trafficking, Smuggling, LA and others.

This bipartite Agreement was signed in a single Technical Cooperation Instrument between Competent Authorities (Prosecutor's Offices of the two States involved) based on the MERCOSUR Framework Agreement.

Joint Investigation Team, signed in October 2020 between the Public Prosecutor's Offices of Paraguay and Brazil, in the area of Human Trafficking, Drug Trafficking and Others.

This bipartite Agreement, constitutes the renewal of the 2019 JIT, but already signed in a single Technical Cooperation Instrument between Competent Authorities (Prosecutor's Office for Paraguay, Attorney General's Office - Prosecutor's Office - for Brazil) based on the MERCOSUR Framework Agreement.

Joint Investigation Team, signed in October 2020 between the Public Prosecutors' Offices of Paraguay and Brazil, in the areas of organized crime, arms trafficking, drug trafficking and others.

This bipartite Agreement, constitutes the renewal of the 2019 JIT but already signed in a single technical cooperation instrument between competent authorities (Prosecutor's Office for Paraguay, Attorney General's Office - Prosecutor's Office - for Brazil) based on the MERCOSUR Framework Agreement.

Joint Investigation Team, signed in November 2020 between the Prosecutor's Offices of Paraguay and Argentina, in the area of LA and others.

This bipartite Agreement was signed in a single Technical Cooperation Instrument between Competent Authorities (Prosecutor's Offices of the two States involved) based on the MERCOSUR Framework Agreement.

2.2. MUTUAL LEGAL ASSISTANCE

150. Mutual legal assistance (MLA), sometimes referred to as "judicial" assistance, is the formal mechanism by which one State, the "requesting State", asks another State, the "requested State", for assistance in obtaining evidence located in the requested State to assist in criminal investigations or proceedings before the courts of the requesting State. Mutual legal assistance is generally based on bilateral and multilateral treaties such as the United Nations Vienna, Palermo and Merida Conventions. However, mutual legal assistance can also take place without a treaty basis.

151. In general, requests should be channeled through the central authorities, e.g. Ministry of Foreign Affairs or Ministry of Justice, and should be drafted in such a way as to comply with the requirements of the treaty and to facilitate the requested State's understanding and compliance with the request.

152. MLA is designed for the collection of evidence, not intelligence or other information. Requests for intelligence/information should be made through informal channels, i.e. contacts between law enforcement officers of the relevant countries. Such informal requests do not involve the issuance of a formal letter of request as in **MLA** requests. That said, informal assistance can, and indeed should, also be used when making evidence collection requests to a State where no coercive power, e.g., a court order, is required to obtain the evidence. Informal information exchange mechanisms reduce the risk of delays and are a useful way of avoiding "fishing expeditions" at the stage of sending a letter of request, as they make it possible to know at an early stage whether or not there is information given in the requested State, for example, information on the existence of a bank account, the movements in that account and the details of the account.

153. In this context, it is important to remember that, although this type of assistance may be characterized as "informal", it does not mean that the evidence obtained is informal or without probative value. This type of exchange of information and spontaneous exchange of information between professionals is enshrined in Article 18(4) and (5) of the Palermo Convention.

154. Prosecutors and investigators sometimes turn to **MLA** without exploring whether informal assistance would meet their needs. The requested State might welcome an informal approach that can be dealt with efficiently and quickly for both parties. Therefore, prosecutors should always ask themselves whether they really need a letter rogatory to obtain a particular piece of evidence. .

155. The extent to which States are willing to assist even with formal requests varies and depends largely on their domestic laws, the nature of the relationship between the requesting and requested State and the general disposition of the officials concerned.

156. Networking among professionals based on trust building is therefore a very important tool to complement **ALM** channels, both in terms of preparing **ALM** requests and ensuring that they are fully implemented, as well as promoting information exchange.

157. Some of the key challenges concern the central authorities, which must be proactive and organize direct consultations between the operating authorities if necessary. In general, it is thought that the best results are obtained when the requesting and requested States have shared draft requests before sending final versions, when requests are actively followed up and when questions from the requested State are answered promptly. In essence, it is better to engage in dialogue rather than blindly sending documents back and forth. The treaty-based assistance system can also be expedited by using technological aids, such as video teleconferencing, and e-mailing advance copies of **ALM** requests.

158. Other challenges relate to the nature of international cooperation itself. Some authorities may choose not to seek formal cooperation such as **MLA** at all if they feel they are unlikely to receive a response. In other cases a bilateral or multilateral treaty basis is lacking or authorities may not even have the necessary knowledge to draft a quality and actionable request, or they may have very rigid standards for seeking international cooperation. Finally, a major obstacle to effective international cooperation is sometimes the lack of a clear political commitment to cooperation, especially when nationals of one country are under investigation in another country.

159. The **letter of request (LoR)** or letter rogatory should provide the requested State with all the information necessary to decide whether assistance should be provided. A major obstacle to **TF/PF** investigations is often the inability of states to make or execute **MLA** requests in a timely and effective manner. Therefore, a level of expertise in international cooperation matters should be developed, as well as international networking among prosecutors and investigators to enable requests, both formal and informal, to be carried out without delay. It is often a good idea to prepare the **LoR** together with experts from the international cooperation unit so that all challenges at the international and investigative level can be addressed. The format and content of an LoR are therefore of fundamental importance, as a poorly written or incomplete request is unlikely to result in assistance. It should contain the legal and practical information summarized below:

- *Assertion of authority by the author of the letter.*
- *Identification of relevant treaties and conventions.*
- *Contact details in the requesting State so that the requested State can make direct contact and clarify issues if necessary.*
- *Guarantees of reciprocity, dual criminality, etc.*
- *Assurances that the material collected will only be used for the purposes set forth in the **LoR**.*
- *Indication of the specific formalities to be complied with in the collection of evidence to ensure its admissibility at trial.*
- *Identification of the accused/suspect.*
- *Status of the investigation or proceeding in the requesting State.*
- *Crimes under investigation or subject to prosecution.*
- *Summary of facts and how they relate to the request. The description of the facts should be sufficiently detailed and should indicate how the requested evidence is necessary for the purposes of the investigation/prosecution.*
- *Necessary consultations and assistance.*
- *Signature of the author of the letter.*
- *Contact foreign authorities and arrange for a draft copy of your proposed MLA application to be sent to them, so that they can advise on the content and wording of the application.*

160. The fundamental differences between **ICS** and **MLA** can be summarized as follows:

ALM	ECI
No investigation in the State of execution.	Parallel proceedings Importance of coordination (common operational objectives and agreement on prosecution strategies).
Limited participation of the requesting authority .	Active participation of seconded members.
Request or response to request Cooperation limited to a specific request Additional measures require a new application or joint initiative with a common purpose	Equal partners; no lead roles, single written agreement.
Information / evidence transmitted after execution of the ALM.	Unlimited exchange of information / evidence in real time.

SPAIN

Agents of the Information Service of the Civil Guard, displaced to Germany, cooperated on December 12, 2017 in the development of a police operation ordered through a rogatory commission by the Central Court of Instruction number 5 and coordinated by the Prosecutor's Office of the National High Court. Several companies and homes in the German cities of Hamburg and Brandenburg were searched for their alleged involvement in a plot aimed at providing financial resources to terrorist groups in the orbit of Al Qaeda. The investigation began on April 22, 2017 when agents of the Intelligence Service uncovered a business plot linked to the financing of terrorism through a company based in El Espinar (Segovia), whose owner recruited two citizens residing in Spain for their illegal activities, and who were all arrested thanks, in this case, to the collaboration of the Egyptian authorities. Investigations revealed the use of a corporate platform established in Spain, managed by two partners, who traded in recycled computer equipment, leaving no trace of their presence in national or international public records. All the resources obtained

from this business activity, according to the investigations carried out, were directly linked to the financing of activities of a terrorist faction linked to Al Qaeda, with the person arrested in Spain having a relevant role in the provision of funds for purposes linked to terrorism. The searches carried out in Germany led to the seizure of abundant documentation related to the economic activity of the companies involved, as well as diverse computer material. The examination of this evidentiary material enabled the investigating officers to confirm the lines of investigation on which this international operation against the financing of terrorism was based. Part of the profits obtained by the activity of the companies of the investigated network was destined to the financing of terrorist groups linked to Al Qaeda, as well as to financially compensate the families of those individuals recruited by the network who joined the aforementioned terrorist groups as fighters. The transnationality of the logistical support and financing networks of jihadist terrorist organizations makes international cooperation between anti-terrorist services essential for the detection of suspicious financial movements and operations, which could be used to finance the activity of terrorist organizations.

3. BEST PRACTICES IN THE FIELD OF INTERNATIONAL COOPERATION TO IMPROVE THE EFFECTIVENESS OF FT/FP ANALYSIS AND RESEARCH

161. Despite the progress made in the region, there are still persistent challenges related to the adoption of an efficient system for the exchange of financial information and intelligence in TF/PF investigations, customs control mechanisms and monitoring of foreign trade transactions that allows for greater cooperation between LEAs, FIUs and Customs and promotes dialogue and cooperation between the competent public and private agencies, in order to implement an efficient and transparent legal regime in the national jurisdictions of the hemisphere. It is vital that there is balance between the creation of regulatory frameworks and the development of strategic operating procedures based on adequate participation and assessment of the different actors involved in the detection, investigation and disruption of these two criminal phenomena. A solid regulatory framework is essential to counteract the challenges and vulnerabilities described throughout this manual, combat TF/PF, discourage criminal activities and favor the institutional and economic development of the countries in the region.

CONCLUSIONS

162. An effective system for combating **FT/FP** requires a comprehensive interagency approach that includes as fundamental elements the identification and involvement of all relevant actors and the establishment of strategic procedures for the detection, investigation and disruption of financial flows linked to terrorism and **WMD** proliferation, including the implementation of a targeted financial sanctions regime that operates along the following lines of action:

- *Strengthening inter-institutional collaboration and information exchange.*
- *Strengthening the traceability of suspicious financial transactions through international cooperation.*
- *Knowledge and specialization on **FT/FP** typologies and the mechanisms for their disruption.*

163. Despite the progress made in the region, there are still persistent challenges related to the adoption of an efficient system for the exchange of financial information and intelligence in **TF/PF** investigations, customs control mechanisms and monitoring of foreign trade transactions that allows for greater cooperation between **LEAs, FIUs** and Customs and promotes dialogue and cooperation between the competent public and private agencies, in order to implement an efficient and transparent legal regime in the national jurisdictions of the hemisphere. It is vital that there is harmony between the creation of regulatory frameworks and the development of strategic operating procedures based on adequate participation and assessment of the different actors involved in the detection, investigation and disruption of these two criminal phenomena. A solid regulatory framework is essential to counteract the challenges and vulnerabilities described throughout this handbook, combat **FT/FP,** discourage criminal activities and favor the institutional and economic development of the countries in the region.

164. Optimizing efforts and mechanisms for preventing, detecting and disrupting **TF/PF** requires the adoption of the following measures:

- *Training in financial analysis and investigation techniques, with particular attention to special investigation techniques.*
- *Prioritize financial investigation and make it a routine part of all investigations into suspected terrorist and/or **WMD** proliferation activities.*
- *Broad and unrestricted access to financial information by **FIUs.***
- *Development and formalization of contacts between **LEAs** specialized in the fight against terrorism and **WMD** proliferation and private sector representatives.*
- *Creation of national bodies dedicated to the identification, tracing, freezing and confiscation of assets linked to terrorism and **WMD** proliferation.*
- *Strengthen the legal and operational capacity of **FIUs** to access banking, administrative and commercial information.*
- *Ensure that a **TF/PF** investigation can be initiated without an underlying terrorism or **WMD** proliferation case, and that the **TF/PF** investigation can continue even when the linked terrorism or **WMD** proliferation investigation has already concluded.*
- *Ensure that financial research linked to **FT/FP** is included in any **JIT** incorporation agreement.*
- *Adoption of a harmonized approach to **FT/FP** risk analysis by **FIUs, LEAs** and Customs.*
- *Collaboration between national agencies and authorities with competence in the **CTF/CPF** fight, allowing constant feedback between each of them to optimize early detection of terrorist groups and proliferator networks.*
- *Creation of a cooperation and information exchange structure involving, in particular, tax authorities, financial supervisory bodies, justice authorities, intelligence services, security services and all relevant administrative authorities in the **CTF/CPF** fight.*
- *Centralization of information on terrorism, **WMD** proliferation and financing.*
- *International cooperation between the **LEAs** and **FIUs** of the countries without delays or administrative barriers in the exchange of information and MLA.*
- *Multilateral legal mechanisms to expedite the freezing and seizure of identified financial assets of terrorist organizations and networks of proliferators.*

165. The handbook on strategic actors and procedures for the detection, investigation and disruption of **TF/PF** is a useful tool to support the efforts of countries in the hemisphere and serve as a guide to address the main national and regional challenges in the fight against **TF/PF,** specifically those related to:

- *Train relevant officials and professionals in **GAFILAT** member states in preventing and combating **TF/PF,** including prosecutors, judges and other relevant criminal justice officials; specialized police; border control and customs officials; financial intelligence analysts; financial institution officials; supervisory/regulatory officials; and compliance officers of selected private sector entities;*

- *Raise awareness of the importance of using special investigative techniques, JITs, legal tools and international guidelines and best practices to efficiently carry out the investigation and prosecution and sanctioning of **TF/PF**, in particular with respect to freezing, seizing and confiscation of financial assets related to ML and **TF/PF**.*

- *Strengthen the legal, regulatory and operational frameworks related to the criminalization of **TF**, freezing, seizure and management of terrorist assets, including those related to designated subjects and entities.*

- *Increase the level of cooperation between the different actors involved in the investigation, prosecution and punishment of **TF/PF** cases, particularly when freezing and seizing terrorist assets.*

- *Strengthen relations between **LEAs**, **FIUs** and Customs at the personal and institutional levels.*

- *Promote greater regional harmonization and national, regional and international cooperation in the fight against **TF/PF** within the framework of international law and the rule of law, especially in the areas of extradition and **MLA**.*

- *Promote a higher level of ratification and effective implementation of the universal and regional legal instruments against terrorism and its financing, the relevant provisions of the United Nations Global Counter-Terrorism Strategy; **UNSC** Resolutions 1267 and successive, 1373, 2178, 2253, 2322, 2368, 2462 and 2482; and the FATF recommendations;*

- *Increase the level of compliance with the recommendations contained in the **CTED** evaluations and in the **GAFILAT** mutual evaluations of the countries in the region;*

- *Enhance the progressive harmonization of legal regimes against terrorism in the hemisphere and strengthen the international legal network to combat terrorism and the proliferation of **WMD** and their financing;*

- *Promote greater transparency in commercial transactions in the region's jurisdictions.*

- *Promote the greater exchange of best practices to minimize **TF/PF** risks.*

- *Promote the exchange of **FT/FP** legislative and regulatory models.*

- *Promote dialogue and inter-institutional cooperation between agencies involved in foreign trade transactions: customs, police, financial intelligence units, and financial and non-financial regulators.*

- *Promote international cooperation to facilitate and expedite the legal movement of goods, services and people.*

- *Raise awareness of the importance of combating FT/FP;*

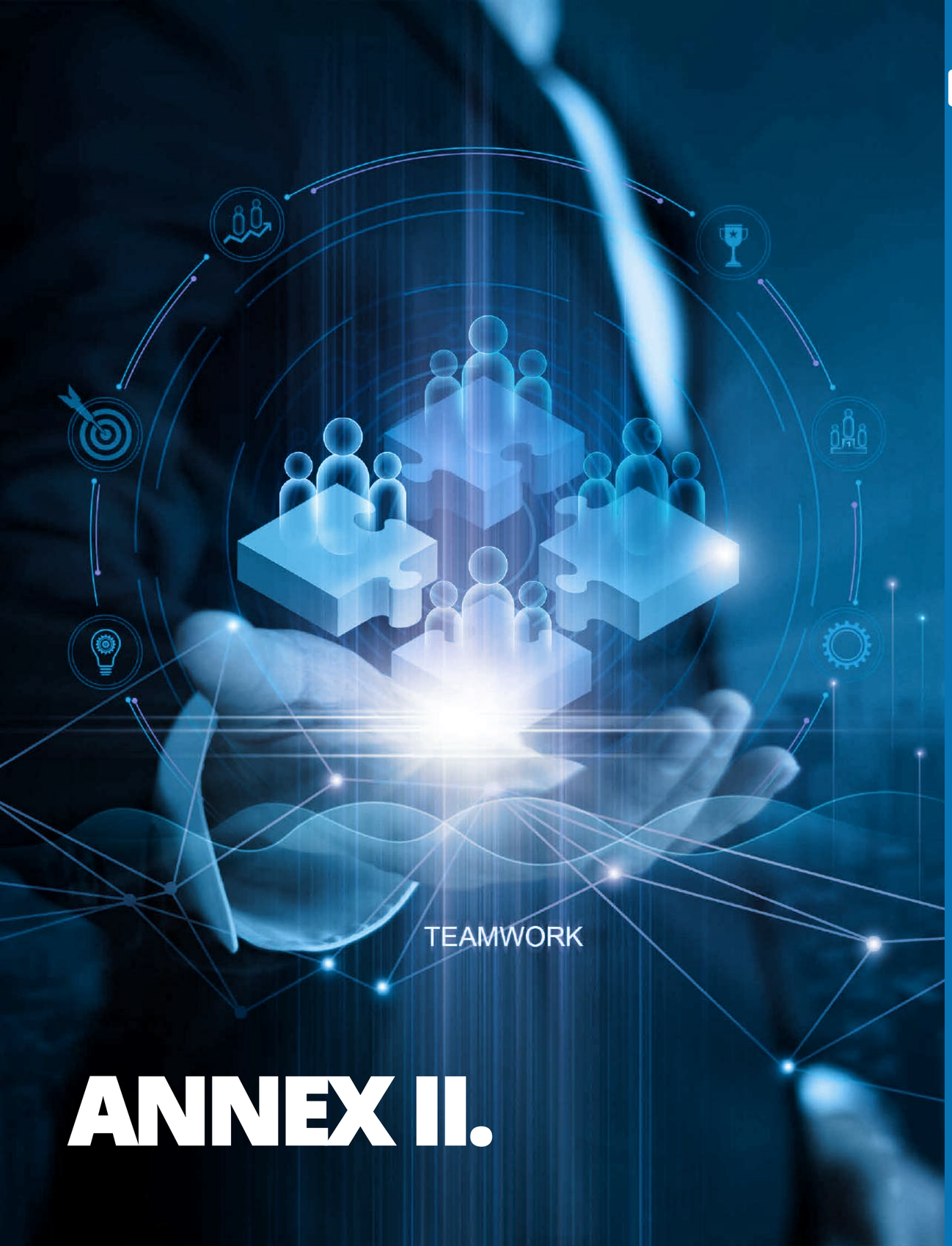
- *Promote greater transparency in commercial transactions in the region's jurisdiction*

ANNEX I.

LIST OF INVESTIGATIONS AND CONVICTIONS IN FT/FP CASES IN GAFILAT MEMBER STATES

COUNTRY	FT/FP RESEARCH	GUILTY VERDICTS FT/FP	PERIOD	SOURCE
Argentina	0	0	Until 2010	2010 IEM
Bolivia	0	0	Until 2018	2018 IEM
Brazil	1	1	Until 2010	2010 IEM
Cuba	2	2	Until 2017	Follow-up Report
Chile	5	0	Until 2010	2010 IEM
Colombia	-	2	2013 - 2018	2018 IEM
Costa Rica	0	0	Until 2015	2015 IEM
Cuba	0	0	Until 2014	2014 IEM
Ecuador	0	0	Until 2011	2011 IEM
El Salvador	0	0	Until 2014	Follow-up Report 9
Guatemala	0	0	Until 2016	2016 IEM
Honduras	0	0	Until 2016	2016 IEM
Mexico	2	1	Until 2018	2018 IEM
Nicaragua	0	0	Until 2017	2017 IEM
Panama	5	5	Until 2018	2018 IEM
Paraguay	0	0	Until 2013	2018 IEM

Peru	7 pre-trial investigations/ 3 ongoing	1	2014 - 2018	2019 IEM
Dominican Republic	0	0		2018 IEM
Uruguay	4	0	2010 - 2018	2020 IEM



ANNEX II.

MODEL AGREEMENT ON THE CREATION OF A JOINT INVESTIGATION TEAM

1. Parties to the agreement

-- ..

2. Purpose of the Joint Investigation Team (JIT)

The purpose of the JIT is to facilitate joint procedural investigation actions in the relevant preliminary proceedings as follows:

The specific objectives of this JIT are:

--

The JIT will develop an operational action plan defining the means to achieve the objectives established in the Agreement.

The Parties to the JIT may redefine by mutual agreement the specific purpose and scope of the JIT.

3. Period covered by the Agreement

The Agreement enters into force on the date of signature by the last of its Parties and is valid for a period of 6 months, which may be extended by mutual agreement. The period of validity indicated herein may be extended.

4. Member States in which the JIT will operate

The JIT will operate in the following member states:

-... y - ...;

The JIT shall carry out its activities in accordance with the law of the Member State in which it operates. If the JIT moves its operational base to another Member State, the law of that Member State shall apply.

5. Head(s) of the JIT

The Parties have designated the following person(s), as representative(s) of the competent authorities in the Member States where the team operates, as heads of the JIT and under whose direction the JIT members shall carry out their tasks in the Member State to which they belong: .....

6. ECI Members

In addition to the persons mentioned in Article 6, the following persons shall be members of the JIT:

Judicial authorities ....;

Police authorities: ....;

Financial intelligence authorities: ....;

....

7. Tests

The Parties shall entrust the heads of the JIT with the task of advising on the collection of evidence. Among their functions is to guide the members of the JIT on the aspects and procedures to be taken into account in the collection of evidence.

8. Internal evaluation

At least every six months, the JIT leaders shall evaluate the progress made towards the overall purpose of the JIT, while identifying and addressing any problems thus identified. Upon completion of the JIT operation, the Parties may, if appropriate, arrange a meeting to evaluate the performance of the JIT. The JIT may draw up a report of the operation, which may indicate how the operational action plan was implemented and the results obtained.

9. Specific provisions of the agreement

The following special provisions may apply between the Parties:

a) *All information legitimately obtained in the territory of the countries where the JIT operates shall be considered as evidence.*

b) *Conditions under which the JIT may request legal assistance under the Convention or other international treaties: requests for legal assistance shall be sent to other States not party to this Agreement, if necessary.*

c) *If the need arises for a Party to the Agreement to send a request for mutual legal assistance to a third State, the requesting State that is a Party to this Agreement shall ask the requested State for authorization for the evidence obtained as a result of the action to be shared with the other Party to the JIT Agreement.*

d) *National legislation on the protection of personal data and protection of classified information, as well as the Agreement between... and .... on mutual legal assistance shall apply.*

e) *Seconded members are not authorized to carry/use weapons in the territory of the State where the operation is carried out, unless otherwise agreed.*

10. Organizational arrangements

a) *The host Member State shall bear the costs of subsistence, accommodation, insurance, intentional travel and written translation of their respective members of the JIT. The evidence shall be translated by the host country.*

b) *Technical equipment: The operational bases of the JIT as indicated in Article 4 of the Agreement are located at .... and at ...The Member State on whose territory the investigative measures are carried out shall be responsible for providing the necessary technical equipment (offices, telecommunications, specific equipment, etc.) to enable the members of the JIT to carry out the missions entrusted to them.*

c) *The official languages of the ECI are..., and...,*

d) *The investigation is subject to Professional confidentiality with respect to all measures and actions taken in... and in... and with respect to the Reports concerning the actions taken, unless the Parties agree otherwise.*

ANNEX III.

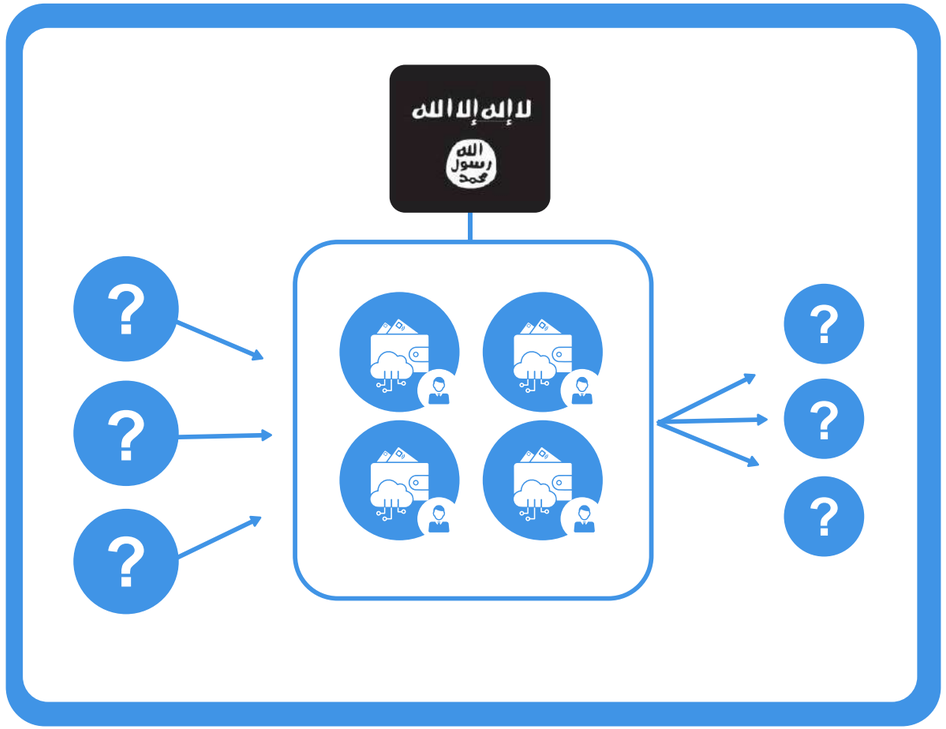
CASE STUDY ON COOPERATION BETWEEN LEA-FIU IN AN FT SCHEME THROUGH E-WALLETS.

The present case study is an example of effective international cooperation between FIUs and national cooperation with **LEAs** in a **TF** scheme through the use of e-wallets. The Russian National Risk Assessment identified, as a top priority, **TF** risks involving financial transactions conducted without having open bank accounts. The common use of the e-wallet payment method by terrorist groups results from the wide geography, speed of the transaction and minimal identification requirements, which therefore complicate the work of analyzing customer interconnections. To reduce this risk, the Federal Financial Supervisory Service (Rosfinmonitoring) pays special attention to the monitoring of financial transactions via e-wallets. The joint investigation resulted in the identification of international **FT** channels and the subsequent suppression of criminal activity. The case was successfully completed within three and a half months from the moment a foreign **FIU** submitted the request for information to Rosfinmonitoring.

STAGES OF THE CASE

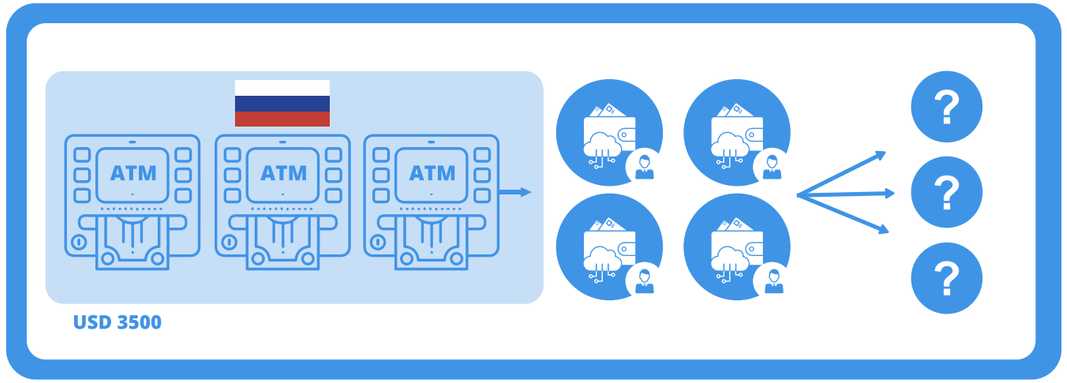
1. EARLY DETECTION

This case was triggered by the request for information received from a foreign partner, the **Financial Monitoring Department (FMD)** of Tajikistan, in January 2017. Based on the information acquired, this **FIU** suspected that 4 (four) e-wallets were related to ISIL financing. The only data available and provided were the unnamed numbers of the e-wallets (+7-XXX-XXX-XX-XX...).



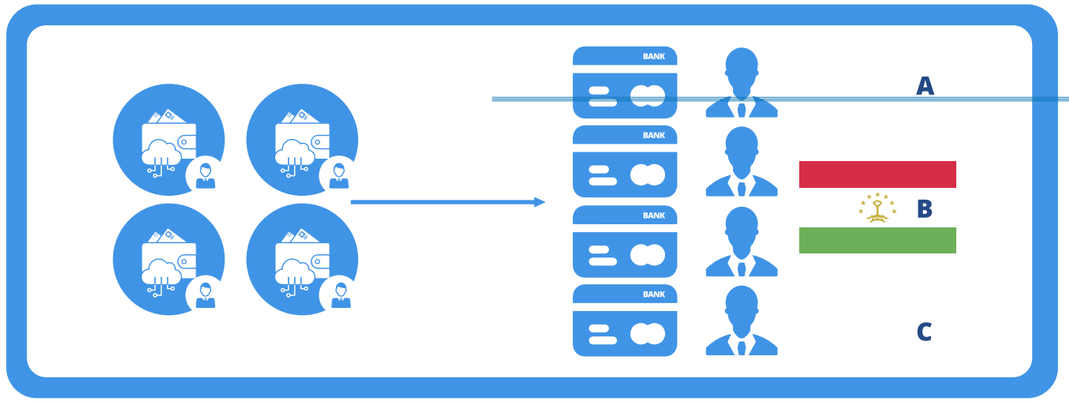
STAGE 1. INITIAL DATA

Rosfinmonitoring started immediately with the identification of the sources of funds and additional cash flows through the e-wallets. Within days, Rosfinmonitoring urged the relevant credit institution to provide the data. The check identified that from April to July 2016, unknown individuals in Russia, through self-service payment terminals, regularly credited e-wallets in small amounts of cash. The total incoming cash flow was RUR 230,000 (≈USD 3,500).



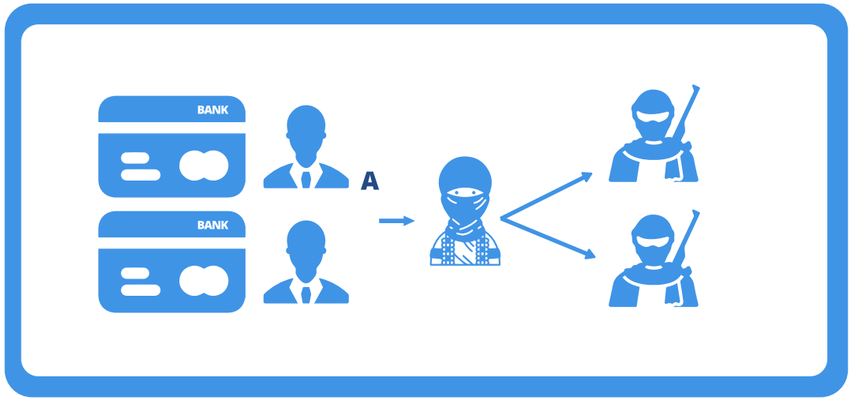
STAGE 2. DATA COLLECTION: INCOMING FLOW.

Rosfinmonitoring scrutinized the debit transactions and identified that the main money flow was through the bank cards of the Russian citizen “Subject A” and 3 (three) foreigners “Subject B”, “Subject C” and “Subject D”.



STAGE 3. DATA COLLECTION: OUTFLOW.

With the prior consent of the requesting foreign **FIU,** Rosfinmonitoring continued the investigation in cooperation with Russian law enforcement agencies **(LEA).** The acquired operational data determined that the subjects had already been suspected of financing terrorist activities. In February 2017, internal cooperation with Russian **LEAs** led to the identification of affiliated persons from the inner circle of the listed subjects, the subjects themselves and other operational information about the controlled persons. Based on

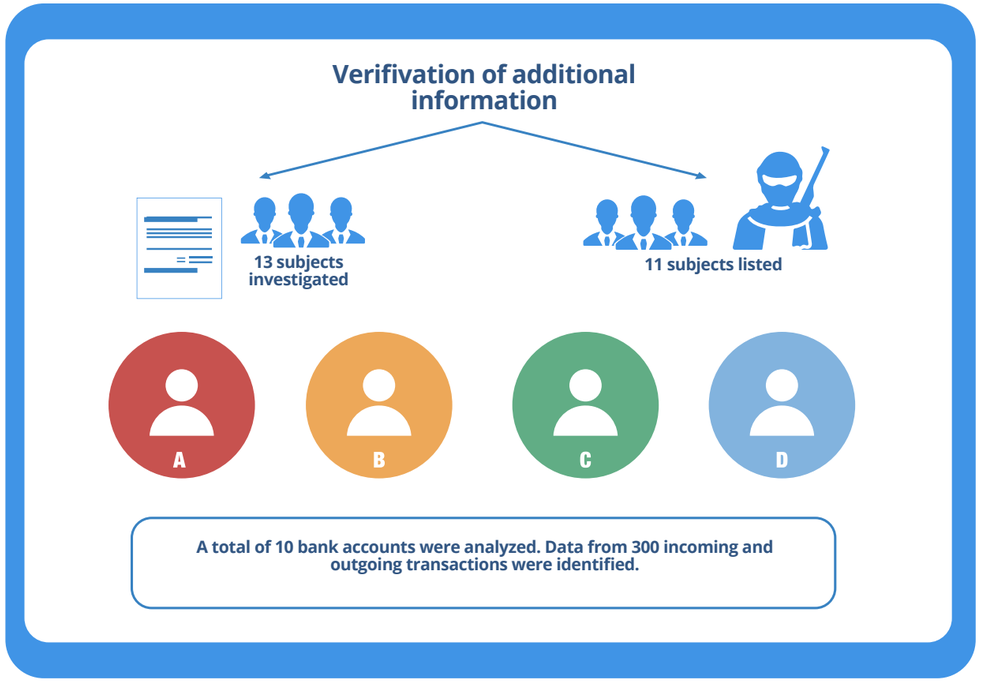


the intelligence received, among the counterparts of "Subject A" and "Subject D", the Russian **FIU** identified an individual who was later (in 2017) placed on the sanctions list for committing an act of terrorism, participating in one of international terrorist organization and conducting propaganda of terrorist activities. In June 2016, the individual credited the account of "Subject A" with RUR 10 000 and the account of "Subject D" with RUR 7000. At the same time, "Subject D" transferred RUR 20,000 to the sister of another listed person, currently wanted for his involvement in the international terrorist organization.

STAGE 4. RESULTS:

NATIONAL COOPERATION IN IDENTIFYING LISTED AND WANTED TERRORISTS

The financial intelligence and information from the LEA was urgently forwarded to the requesting FIU. In March 2017, the requesting FIU added additional information to the intelligence held by Rosfinmonitoring and identified the owner of the bank card credited from the e-wallets as "Subject B", a member of ISIL fighting in Syria. Further bilateral analysis of Subject A's private connections revealed an individual wanted by both countries for offences related to the formation of an organised criminal group and an extremist group, as well as illegal arms trafficking. In June 2016, Subject A transferred 5000 RUR to this wanted individual. A review of the cash flow of the accounts described another contact of "Subject B". In October 2016, the contact transferred around RUR 30 000 to "Subject B" through two (2) separate transactions. At the time of the investigation of the case, the individual was already on the sanctions list and was being prosecuted for his involvement as a terrorist fighter in Syria. A joint national in-depth investigation of the bank statements of "Subject C" revealed:

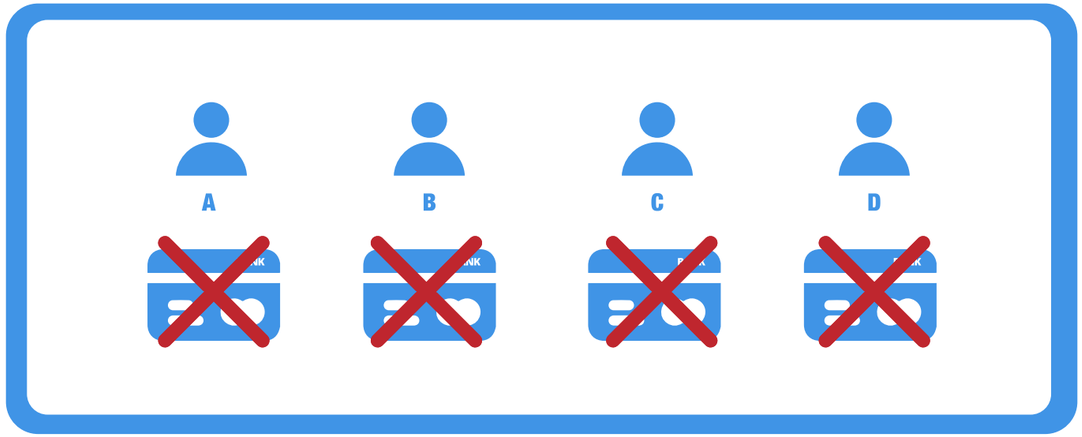


STAGE 5. RESULTS: ADDITIONAL INTELLIGENCE

Additional intelligence provided to the Tajikistan **FIU** in March 2017

- *13 individuals whose assets were already frozen as a result of parallel investigations (after they completed the transactions described in this case).*
- *11 individuals already listed after the initiation of criminal cases under articles related to terrorist activities as a result of parallel investigations (after they completed the transactions described in this case).*

This intelligence was forwarded to the partner **FIU** for immediate action. In April 2017, under the "Mutual Asset Freezing Project" of the participating countries' FIUs, the assets of Subjects **"A", "B", "C" and "D"** were frozen by the Russian **Interagency Committee for Countering the Financing of Terrorism (ICCTF)** on the basis of sufficient grounds for suspicion that these subjects were engaged in activities potentially related to **TF.**



STEP 6. RESULTS: FROZEN ASSETS. END OF CASE

The **ICCTF's** decision to freeze the assets of foreign individuals, Subjects **"B", "C" and "D",** was immediately forwarded to the Tajik **FIU.** Access to the Russian financial system was blocked for all subjects by sending a special notice to all reporting entities. Rosfinmonitoring will receive an alert if the Subjects attempt to open a new account at another credit institution. Based on intelligence provided by Russia, the partner **FIU** initiated criminal cases against Subjects **"B" and "D"** for offenses related to terrorist activities and **TF.**

FINAL STAGE. CONCLUSION: EFFECTIVENESS OF JOINT INFORMATION EXCHANGE IN BILATERAL RESEARCH.

The case benefited from and contributed to the "Mutual Freezes" project carried out by Rosfinmonitoring within the Global **CFT** network. In order to prohibit the illicit use of the financial systems of participating countries, Rosfinmonitoring exchanges lists of **TF** suspects with counterpart **FIUs.** The **ICCTF** assesses their adequacy and sufficiency and approves the freezing of assets.

BIBLIOGRAPHY

- *Brewer, Jonathan. 2017. Analysis of Typologies of Financing the Proliferation of Weapons of Mass Destruction. Kings College, London.*
- *World Bank. 2008. Anti-Money Laundering and Combating the Financing of Terrorism. Comprehensive Training Guide. World Bank. Washington DC.*
- *World Bank. 2007. Anti-Money Laundering and Combating the Financing of Terrorism Reference Guide. Second edition. Schott, Paul Allan. World Bank. Washington DC.*
- *United Nations Security Council. 2019. "Technical Guide for the Implementation of Security Council Resolution 1373 (2001) and Other Relevant Resolutions." S/2019/998. https://www.undocs.org/es/S/2019/998.*
- *United Nations Security Council. 2020. Joint report of the Counter-Terrorism Committee Executive Directorate and the Analytical Support and Sanctions Monitoring Team pursuant to resolutions 1526 (2004) and 2253 (2015) concerning the Islamic State in Iraq and the Levant (ISIL, also known as Da'esh), Al-Qaida and the Taliban and individuals, groups, undertakings and entities associated with them on measures taken by Member States to impede the financing of terrorism, prepared pursuant to paragraph 37 of Security Council resolution 2462 (2019). S/2020/493. https://undocs.org/es/S/2020/493*
- *FATF. 2012. Guide for Financial Investigations. FATF/OECD. Paris*
- *FATF. 2012-2021. International Standards on Combating Money Laundering, Terrorist Financing, and Financing the Proliferation of Weapons of Mass Destruction. FATF/OECD. Paris*
- *FATF-Egmont Group. 2020. Trends in Trade-Based Money Laundering. FATF/OECD. Paris*
- *FATF 2018. Implementation of the Financial Provisions of the United Nations Security Council Resolutions to Combat the Proliferation of Weapons of Mass Destruction. FATF/OECD. Paris*
- *FATF 2018. Implementation of the Financial Provisions of the United Nations Security Council Resolutions to Combat the Proliferation of Weapons of Mass Destruction. FATF/OECD. Paris*
- *FATF. 2018. Financing of Recruitment for Terrorist Purposes. FATF/OECD. Paris.*
- *FATF, 2010. Money Laundering Vulnerabilities in Free Trade Zones (FTAs). FATF/OECD. Paris.*

- *GAFILAT, 2018. Best practices in cross-border cash and securities transportation monitoring. GAFILAT. Buenos Aires.*

- *GAFILAT, 2019. Report of results regional workshop on trade-based money laundering (TBML) held in Panama City, Panama, April 3-4, 2019. GAFILAT. Buenos Aires.*

- *GAFILAT. 2021. Best Practices on procedures and/or mechanisms for domestic designation or execution of third country orders in line with UNSCR 1373. GAFILAT. Buenos Aires.*

- *Golobinek, R. 2006. Financial Investigations and Confiscation of the Proceeds of Crime: A Training Manual for Law Enforcement Agencies and the Judiciary. Council of Europe. Strasbourg.*

- *Egmont Group. 2018 - 2019. Annual Report. Egmont Group. Toronto.*

- *Egmont Group. 2017. Operational Guidance on the Performance of Financial Intelligence Units and Information Sharing. Egmont Group. Toronto.*

- *STAR Initiative. UNODC. World Bank. 2018. Financial Intelligence Units working with law enforcement agencies and prosecutors. World Bank. Washington DC.*

- *OECD. 2019. Money Laundering and Terrorist Financing. Handbook for Tax Inspectors and Auditors. OECD. Paris.*

- *OECD. 2012. Effective inter-agency co-operation in the fight against tax and other financial crime. OECD. Paris.*

- *OAS. 2007. Practical Guide for the Prevention, Detection and Suppression of Terrorist Financing. OAS. Washington DC.*

- *OAS. 2017. Technical Evaluation-Comparative Analysis of Typologies and Patterns of Money Laundering and Terrorist Financing in Three Latin American Free Trade Zones. OAS. Washington DC.*

- *WCO - Egmont Group. 2021. Manual on Cooperation between Financial Intelligence Units and Customs. WCO. Brussels.*

- *UNODC. 2018. Guidance Manual for Member States on Terrorist Financing Risk Analysis. UNODC. Vienna*

- *UNODC. 2014. Guide for Colombia on the Legal Regime against Terrorism and its Financing. UNODC. Bogotá.*

- *UNODC. 2014. Investigation Plan for the Crime of Terrorist Financing in Colombia. UNODC. Bogotá.*

- *Yansura, J.; Mavrellis, C.; Kumar, L.; Helms, C. 2021. Financial crimes in Latin America and the Caribbean: Understanding country challenges and designing effective technical responses. Global Financial Integrity. Washington DC.*

GAFILAT