A Target-Centric Intelligence: How Efficient is Cooperation Between the Local Police Departments and the FIU within the Finnish AML/CTF model?

August 2019

Student IDs
University of Glasgow: 2234303
Dublin City University: 17116147
Charles University Prague: 63296380

Presented in partial fulfilment of the requirements for the Degree of International Master in Security, Intelligence and Strategic Studies

Abstract

This research intends to address the issues of cooperation and intelligence sharing between the national authorities within the network of Anti-Money Laundering and Counter-Terrorist Financing regime. In this way, it is aimed to better understand and analyse the underlying issues behind the gaps in effective operational exchange of financial intelligence information within the wider network of national security structures. Therefore, this work contributes to a highly varying and inter-disciplinary academic field of studies on AML/CTF but also wider to the researches on security, terrorism and crime prevention. The academic debates on the methods of measurement of effectiveness of the AML/CFT models has developed a range of different perspectives, which have certain constraints and limitation for analysis. The traditional approach of evaluation relies heavily on the outcome-orientation and, therefore, is not always able to identify the weaknesses on the operational level and related processes. This approach is especially in use in the contemporary official evaluations and assessments of AML/CTF regimes. In this way, this dissertation applies a theoretical framework of a "target-centric" intelligence and tries to go deeper into the intelligence sharing processes to supplement the recent FATF analysis on Finland.

Table of Contents

Table of Figures

Chapter 1: Introduction and Outline of the Research

Justification

Money laundering and terrorist financing (ML/TF) are illegal activities that pose a significant threat to various dimensions of national and international security in a contemporary globalised world. Given its complicated and discreet nature, ML/TF is usually seen (Unger 2013, p. 20) as a victimless or secondary crime in comparison to drug trade, terrorist attack, human trafficking, kidnapping, and other more violent crimes that dominate the headlines in media. This observation is supported by the fact that the first international measures to tackle such activity were taken only 30 years ago with the establishment of Financial Action Task Force (FATF) in 1989. FATF is coordinated
by the OECD in Paris but is still and independent standard setter, which is now considered as one of the main international organisations in the field of anti-money laundering and counter-terrorism financing (AML/CTF) (Schott 2006, pp. III-7-III12).

However, through more detailed analysis it becomes evident that ML and TF form a backbone of every serious criminal enterprise and thus require detailed attention from security professionals and academic researchers. The strategic importance of ML/TF lays in its operational framework that brings together different illicit actors such as terrorists (Keene 2012, pp. 271-366), cyber criminals and hackers (Ibid, pp. 143-270), organised criminal groups (Campbell 2019), corrupt officials (Garside 2019), human traffickers (Lake 2015), and illegal wildlife traders (Thomas 2019) to mention a few. Combined together these crimes are a serious challenge to any government and the international community in general as they undermine security and create a vicious cycle that can penetrate every field of state and society. ML/TF is an Achilles' heel of the criminal threat and targeting this heel can help to prevent and disrupt further growth of wrongful behaviour. Even if ML/TF includes large quantity of methods to move criminal funds (Reuter & Truman 2004), its ultimate objective is constantly the same: to hide criminal origins of financial assets and additional investment in illegal operations. Consequently, an effective anti-money laundering and counter-terrorism financing regime could not only supplement criminal investigations and trials but also serve as a tool in identifying and preventing illicit actors in their undertakings.

Despite the formidable growth of international and national attempts to fight money laundering and terrorist financing, the current situation is still far from ideal. Recent scandals of "Global" Laundromat (Harding 2017; Garside 2019) and leaks of "Panama"/ "Paradise" papers (Bernstein 2017) demonstrate well how relatively easy it is for criminals to avoid detection from authorities. These documents are

related to the offshore jurisdictions and the law firms, which were providing corporate services that were also widely used for illegal purposes. While the papers have caused various political scandals and investigations (BBC, 2018), these leaks lead to a conclusion that there are still multiple gaps in the international AML/CTF, and more work needs to be done. Moreover, the mentioned examples are just the peak of an iceberg as even careful estimates show a figure of approximately 0.8 – 2 trillion USD being laundered yearly worldwide (UNODC 2019), and situation is not likely to change with a growing threat of organised crime and terrorism (EUROPOL 2019).

The steady flow of exposures of ML/TF cases in the US, EU, and other parts of the globe raise the question of how effective are the national and international AML/CTF regimes and how could they be improved to meet the requirements in their given tasks. Taking into consideration the global scale of the problem, different security environments, and national responses, the question of effectiveness is not easy to answer as the eventual outcome depends on the applied perspective and theory. The research topic of (A)ML/(C)TF is composed of multiple elements with various influential factors that complicate the development of unified methods of analysis. This research project will focus on the important issue of inter-organisational cooperation and the flow of intelligence between financial intelligence units and local police departments. The main goal is to concentrate on a national level and assess the efficiency of cooperation; identify the existing obstacles and problems; and provide recommendations for potential improvement of the chosen model.

Cooperation matters are not new in security studies and there is a growing amount of literature related to intelligence (Shiraz 2013), law enforcement (Alpert and Dames 2011), counter-terrorism (D'Souza 2008), and other forms of combined efforts to tackle various threats including in their financial dimension. Increasing interest in topics of cooperation can be explained by the inability of a state or any organisation to face contemporary security challenges relying solely on its own capabilities. Especially in AML/CTF, where criminal tentacles are widely spread and can emerge on all levels of a financial system, simultaneously crossing multiple international and national jurisdictions. Therefore, effective counter-measures require sophisticated network of organisations that could form a single mechanism in a national security environment. However, as it often occurs, established partnerships can face various challenges that complicate the efforts to reach shared objectives and potentially affect the operationality of the whole network (Prezelj 2014). In AML/CTF models, Financial Intelligence Units (FIU) are a central point of contact between public and private sectors, and their tasks include gathering, analysis, and dissemination of financial intelligence to relevant organisations. At the same time, Law Enforcement Agencies (LEA) are responsible for conducting investigations and preventing further crimes, and, thus, an uninterrupted flow of information is required between LEAs and FIUs.

Research Question

This study will focus on the Finnish AML/CTF model where, according to the recent FATF (2019a) mutual evaluation report, cooperation between the local police departments and the financial intelligence unit is insufficient and requires further improvement. The report does not provide explanation of underlying reasons and obstacles for effective communication or any recommendations for necessary actions. In addition, the author of this work has necessary language skills, regional knowledge and working experience in the Finnish government structures such as the Helsinki Police Department and the Finnish Immigration Service. Therefore, this research will fill the gap in knowledge of identified problem and provide instruments of analysis for further researches in other countries with a similar AML/CTF system. The result of this study could benefit the professionals working in the field and provide practical solutions for more effective coordination of their actions. Consequently, the research aims to answer the question: **How efficient is the flow of information and cooperation between the local police departments and Financial Intelligence Unit within the Finnish AML/CTF?**

Theoretical Framework

This research project falls into the scope of qualitative analysis and will engage with various sources of information to build a holistic and analytical review of the current situation in the Finnish AML/CTF with a particular emphasis on cooperation matters between the FIU and local police departments. Therefore, this analysis will supplement a recent FATF mutual evaluation report and go deeper into various AML/CTF models that were addressed in previous research. The aim is to understand the outcomes of report and apply critical analysis for its assessment. Although the research field of AML/CTF is undermined by insufficient empirical data and limited access to primary sources, there is good number of official documents that will be analysed through the lenses of security and intelligence studies to identify factors potentially influencing on intelligence sharing. In order to measure the efficiency of cooperation between FIU and LEAs this research aims to answer the following sub-questions in a similar order throughout the research paper:

1. What are the characteristics of the Finnish security environment regarding dominating predicate crimes and terrorist threat?

2. What is the structure of the Finnish AML/CTF model and how does it align with the contemporary security environment?

3. What are the main tasks, responsibilities, and intelligence needs of the FIU and LEAs? What sort of financial intelligence does FIU gets access to or generate and how does it share this intelligence with the partner organisations?

4. How does cooperation of FIU and local police departments fit in a broader terrorist and crime prevention strategy?

5. How and what factors influence intelligence sharing and cooperation in this context?

Structure

The rest of this chapter is devoted to introduce the reader to the main definitions related to money laundering and terrorist financing, as well as go through the main studies in the field of AML/CTF. Further, this dissertation includes three additional chapters, which aim to consistently outline the main points and cumulate knowledge before the final analysis of the main research questions. In this way, the second chapter will look at the major developments on the international, regional and national levels to equip the reader with the necessary information about the elements in contemporary AML/CTF practices. AML/CTF related documents and organisations will be discussed to narrow the attention to national states and different security models. After presenting the general trends, the attention will be shifted to the Finnish security environment and variation of the AML/CTF structure. The aim is to identify relevant legislation, practices and organisations in anti-money laundering and counter terrorist financing. Finally, the last chapter is the main analytical body of this work. There, this dissertation will operationalise the concept of a "target-centric" intelligence and approach the operational issues regarding the cooperation and intelligence sharing between the financial intelligence unit and the investigative authorities within the AML/CTF network and wider national security structure. Finally, the outcomes of the analysis will be assessed in light of the FATF report and final conclusion will be made on the efficiency of the flow of information and cooperation between the local police departments and the FIU.

Main Terms and Definitions

From a legal perspective, money laundering can have many definitions depending on the jurisdiction and the state's historical, economic, and criminal context (Utrecht University 2013, pp. 12-28). In simple terms money laundering is "the processing of the criminal proceeds to disguise their illegal origin" (FATF 2019b). As a result, money laundering is always related to a predicate crime, such as drug trade or

human trafficking, that generates a large amount of illegal income and creates a need to integrate these funds back into legal economy. Usually, the process of money laundering is divided into three main steps that are "placement", "layering", and "integration" (Cassara & Jorisch 2010, pp. 9-17). Through these simplified concepts it is easier to understand the complex stages of ML and separate them for an analysis.

Placement is a first step and it is the most vulnerable for detection. At this point, criminals try to place their illegal incomes in accessible financial instruments and create a basis for money flows across economic systems. The most straightforward example is a drug dealer trying to deposit his earnings in banks to turn significant amount of cash in more convenient form of financial assets. Layering means actions taken to distance the money from the crime that could be in form of multiple bank transaction across the national borders, where the drug dealer tries to prevent authorities from tracing his funds. Finally, integration is a stage where criminals invest their seemingly legitimate funds back into economy by utilising such opportunities as investment in real estate, arts, luxury products, or businesses to benefit from the dirty money. It is worth to mention that there are multiple variations of ML schemes depending on a type of predicate crime or available opportunities for the criminal actors and in some cases certain steps (placement for example) can be avoided (Koningsweld 2013).

Terrorist financing is in many ways similar to money laundering as there is a strong link between terrorism and crime (Makarenko 2004). This correlation means that terrorists and their supporters can benefit from the same sources and methods to access illicit funds. In addition, similar to criminal actors, terrorists try to remain discrete regarding their funds and its link to terrorist purposes. However, terrorist activity, contrary to organised crime, is not only aimed to generate funds but attracts money to meet the financial requirements for terrorist operations and to cover broader organisational costs (FATF 2019c). In this way, terrorists can also raise funds from legitimate sources and state sponsors (Ibid), which complicates the work of law enforcement and intelligence agencies.

To tackle these crimes and activities, states have established national AML/CTF regimes and deepened their cooperation through the platforms of regional and international organisations such as the United Nations or the European Union (Schott 2006, pp. III-1-IV-9). An AML/CTF regime can be defined as a framework of legislation, norms, practices, and organisations that are implemented to safeguard a national economy and financial institutions from a toxic flow of dirty money. These regimes also form a basis for gathering, analysing, and disseminating financial intelligence in order to provide law enforcement and security professionals with crucial information for further actions. An AML/CTF network includes various government bodies and private sector representatives with specific tasks related to their field and type of responsibilities within a state hierarchy. Each organisation within such networks has important

roles but also limitations in terms of meeting the demands of preventing and disrupting ML/TF. For example, a tax office may have its own tools to identify cases of tax evasion but might not able to detect drug traders. Law enforcement officials are sometimes dependent on information from the private sector, that is legally obliged to provide data about suspicious activities in their business areas. Therefore, inter-organisational cooperation is essential to the effectiveness of the whole system.

At the centre of any AML/CTF model and broader counter-terrorism and crime prevention strategies is financial intelligence, which can support criminal or intelligence investigations by providing information on money flows from criminal sources. Financial intelligence can be valuable on its own and draw the attention of security agencies on suspicious transactions and financial activities that could eventually expose criminals and terrorists. This research will adopt former (US) Assistant Secretary of the Treasury for Terrorist Financing and Financial Crimes Juan C. Zakarte's approach (2013, p. 77) who defines financial intelligence as "any bit of information—however acquired—that reveals commercial or financial transactions and money flows, asset and capital data, and the financial and commercial relationships and interests of individuals, networks, and organizations". Such a broad definition is particularly useful for a wide analysis of an AML/CTF model aiming to counter highly varying and to an extent unpredictable criminal behaviours.

Finally, security measures do not exist in a vacuum and are shaped in accordance to the threats seek to tackle. Therefore, this security environment (Tang 2007) has a decisive influence on the allocation of scarce resources and formulation of strategic objectives. In the AML/CTF landscape, similarly to traditional national security, chosen tactics and strategies should be constantly updated depending on strengths and capabilities of an adversary in form of criminals and terrorists. Every country has its unique features and challenges that limit and simultaneously provide various opportunities for ML/TF operations and, thus, determine priorities for law enforcement and intelligence agencies. Conclusively, the AML/CTF environment encompasses illicit actors, methods, vulnerabilities, and available resources related to the realities of national, regional, and international frameworks. While criminal actions are not static -- it is unavoidable that methods will become more creative in order to avoid unwanted attention -- a recognition of the specific nature of each security environment can increase the effectiveness and precision of AML/CTF efforts.

Literature review

Money laundering, terrorist financing and related topics have been studied from various approaches in different disciplines. Since ML/TF is highly complicated in nature and brings together many aspects of

crime, security, international relations and other fields, a variety of works are important to generate deeper knowledge and understand the processes happening in the criminal environment. Criminals are constantly adopting their methods in accordance to national and international responses, and states have to follow up with the changing trends. Understand the methods of AML/CTF also requires a good grasp of the threat landscape and related issues such as predicate crimes, actors, the scale of the threats and their consequences, and loopholes in the contemporary security system. Altogether, the academic community has produced a large amount of research on ML/TF.

The threat of money laundering and terrorist financing poses a danger to states and societies. A wide range of scholars and organisations have tried to measure how harmful ML/TF is and who actually suffers from this activity. The academic literature suggests that ML/TF can have direct and indirect negative effects economically, socially, and politically (Ferwerda 2013, pp. 35-38). Scholars have showed that money laundering and terrorist financing can increase levels of crime (Serio 2004), fuel the spread of corruption and bribery (Armey and Melese 2018), undermine the integrity and reputation of financial system (Bartlett 2002), support terrorist movements (Rudner 2010), and by implication create a basis for more serious consequences such as the spread of weapons of mass destruction (FATF 2008). All these works are useful to realise the risks and justify the costs of AML/CTF, since every crime eventually has to have a victim that makes it harmful in the eyes of public and justice (Groot 2013). However, Joras Ferwerda (2013) rightly points out that the main problem with academic research in this field is that it is undermined by insufficient empirical evidence and research material, which leaves many of the estimates on the side of speculations. While Ferwerda touches upon the important question of available data, there is no reason to under-evaluate the issue as even the "second chance for law enforcement" (Ibid, pp. 38-39) to disrupt the toxic flows of money, and, therefore, dismantle terrorist and criminal organisations is valuable enough to bear the costs of AML/CTF.

Academic studies regarding the nature of ML/TF are supplemented by analyses of vulnerabilities and the scale of the problem. Peter Reuter and Edwin M. Truman (2004) accentuate that such estimates are necessary to guide policymakers and allocate resources to more problematic and vulnerable financial sectors to ML/TF. In this particular task researchers have mostly relied on economic approaches and developed a number of models to measure the threat on the global (Walker and Unger 2013) and national levels (Bagella, Busato and Argentiero 2013). Based on the amount of suspicious transaction reports (Harvey 2004), estimates of illicit financial flows (UNODC 2011), or analysis of "grey economy" (Kommer 2013), it is possible to shed a light on approximate figures of dirty money and loopholes in the international financial system. The most notable example are the estimates of UNODC (2011) in which dirty money forms around 2-5% of global GDP. Moreover, case studies (Marat 2015) on specific states

can help to identify major risks and typologies of ML/TF to help identify pathways to strengthen international and domestic inter-agency cooperation. However, terrorist financing poses a particular research problem for a global measurement because of its different objectives and partly legal sources of funds that are difficult to separate from the healthy financial transactions. Case studies on regional level regimes (Croissant and Barlow 2007) and particular terrorist groups (Rudner 2010) are a predominant choice for researchers in this field.

Due to a large number of theoretical frameworks and the use of different databases, there is no consensus on what methods are most reliable to study (A)ML/(C)TF topics as many of them suffer from various drawbacks. For example, both the United Nations Office on Drugs and Crime and Financial Action Task Force use information provided by the member states, and might receive manipulated material for political reasons. Moreover, a comparison of national statistics is problematic as every country has distinct legislation, compliance requirements, criminal environment, reporting procedures, and AML/CTF structure. From this perspective, the question of effective international AML/CTF is strongly related to every individual state's capacity and political will to eliminate ML/TF from its jurisdiction (McCarthy 2013).

While a general overview of potential threats and illicit flows helps to understand the problem in general, money laundering and terrorist financing are notable for the diversity of their forms, participants and settings. It is futile to expect that criminals and terrorists will always follow same patterns in hiding their money. Their adaptability creates a need for detailed knowledge about their methods and illicit markets. Broadly speaking, ML/TF forms a complicated web at the intersection of legal and illegal dimensions. Every string of this web has particular characteristics depending on a predicate crime that determines the ways of certain laundering tactics. Heavily cash dependant drug dealers may rely on cash smuggling, gambling, structuring, and cover business whilst terrorist might use charities and "hawalas" (informal banking system) to move money to conflict zones. This issue is widely acknowledged in academic and professional circles which have produced studies on specific methods (Hunt 2011), general trends (Morris-Cotterill 1999), emergence of new payment systems (Stokes 2012), and detailed analyses of predicate crimes (Levi 2013). In addition, FATF (2018) has recently released a study on professional money launderers where an in-depth overview of ML services and actors is made available to the public for the first time.

Despite the large amount of literature, every aspect of ML/TF is still debatable, which makes it difficult to develop a comprehensive set of counter-measures. Specifically, the measurements of effectiveness and efficiency of AML/CTF have been under scrutiny, Levi, Reuter and Halliday (2018) highlight differing

interpretations and perspectives on them. A lack of exhaustive theoretical knowledge and empirical data raises the question of how to assess something that is unknown? If an FIU manages to freeze 1,000,000€ then how much money was laundered? If CTF aims to prevent terrorist attacks then how many of them did not actually happen? Moreover, AML/CTF and financial intelligence formulate only part of the complicated security networks (Prezelj 2014, p. 326) and it remains unclear to what extent successful crime and terrorism prevention is dependent on such measures.

At this point, as it is outlined by Barbara Vettori (2013), there are two general approaches to the study of AML/CTF: traditional and new assessment methodologies. Traditionally, an analysis of an AML/CTF and its effectiveness has been done through the evaluation of outcomes across the set standards of effectiveness. This methodology is particularly common in official evaluations done by FATF (and other organisations) that aim to develop universal AML/CTF standards and follow implementation of required policies in its member states. The evaluation process relies on national statistics coming from (Ibid, p. 475): 1. suspicious transaction reports; 2. number of investigations, prosecutions, and convictions including on property frozen, seized and confiscated; 3. legal assistance and international requests for cooperation; and 4. on-site examinations (e.g. interviews). Gathered material is then compared to existing requirements such as FATF 40+9 recommendations (FATF 2019d) to identify whether an AML/CTF model has been structured accordingly. In addition, FATF member states are encouraged to conduct national risk assessments to keep track of changing trends in their jurisdictions and take necessary steps further. In this way FATF "mutual evaluation reports" provide the most comprehensive insights on national AML/CTF regimes, and their current status is discussed based on key topics such as legal system and supervision mechanisms (FATF 2019a).

This traditional perspective has been criticized for its overreliance on policy analysis and the instrumental side of AML/CTF, leaving aside potential consequences and the impacts of the system under study. Critical voices question whether AML/CTF is reaching its objectives of reducing the level of crimes (Ferwerda 2009), prevent terrorist attacks (Brzoska 2016), effectively fight global "public bads" (Reuter & Truman 2004), and bring criminals to justice (Vettori 2013). "New assessment methodologies" that apply methods of cost-benefit analysis to estimate the extent to which AML/CTF requirements are beneficial compared to the costs created for the private sector (Sathye 2008) and taxpayers (Reuter & Truman 2004). By questioning traditional assessments and putting official statistics into another perspective, alternative researches contribute to discussions on AML/CTF efforts. The potential impact of AML/CTF policies is worthy of interest since it could form an obstacle for a state to take such actions (MONEYVAL 2015).

Analysing outcomes and impacts do not necessary provide insights on problematic spots in the system itself. Our main assumption is that inability to reach sufficient performance in AML/CTF and establish uninterrupted flow of financial intelligence might actually hide in details as, for example, in inefficient public-private cooperation (Maxwell and Artingstall 2017). Therefore, an effective security mechanism requires functionality in all of its elements and strong intelligence capacity. In intelligence studies, the role and circulation of information is usually approached from the perspective of policymakers and their intelligence needs (Scott and Jackson 2004). In the traditional framework intelligence is represented in the form of a cycle that starts from consumers' needs and by going through several stages generates a final product, ideally in a timely and accurate manner (Johnson 1986). Additional characteristics of "good" intelligence include relevance, usability, reliability, and validity depending on an issue at the moment. Nevertheless, intelligence gathering, analysis and dissemination become more complicated when there are multiple consumers with varying intelligence needs (Clark 2013, pp. 80-90). In this situation organisations working together on a same target or objectives have to structure their cooperation in a supplementary way to meet the requirements.

Coming back to AML/CTF models, it is possible to notice that there is a linear structure with diverse objectives set for each organisations and, therefore, intelligence needs are formulated in accordance to their respective tasks and responsibilities. These organisations belong to multiple networks simultaneously and their information comes from a number of sources including some that are outside of the AML/CTF network (Carter 2009, p. 11). As a result, to take this complex landscape into account, the proposed research should be formulated in a way that highlights how where and what sort of information is going through the established channels. Ioana Deleanu (2013)'s analysis of "the role of information for successful AML policy" evaluates different flows of information in three types of financial intelligence units (administrative, judicial, law enforcement). Through a framework of collaborative filtering approach and prosecutor services as "the end-users", Delenau managed to identify the strengths and weaknesses of each AML settings, and most importantly FIU's access to various databases. Delenau proposes a "hybrid" type of FIU that would maximise intelligence collection and analysis for effective prosecution. Her work is then expanded further as a part of an EU-wide "ECOLEF" project (Utrecht University 2013) on "the economic and legal effectiveness of anti-money laundering and counter terrorist financing policy". Although to an extent similar to FATF evaluation reports, this project demonstrates well the unique characteristic of national information transmission chains and varying differences among institutions.

The evaluations of FATF, Delenau/ECOLEF, and other researchers working on effectiveness of AML/CTF all emphasise the centrality of FIUs. The powers of FIUs will be discussed later in the research but at this point it is worth to mention that FIUs are mostly passive actors in the network and

operate with information provided by other parties (IMF 2004, pp. 32-70). In this way, FIUs have reactive approach to terrorism and crime prevention and mainly draw the attention of other security agencies on suspicious elements. On the contrary, law enforcement agencies include reactive and proactive approaches, they investigate crimes that already took place and prevent new ones from happening. Moreover, LEAs have a broad set of tools for collection of intelligence and FIUs form only one valuable source of financial information. Therefore, evaluations of FIUs performance and cooperation with any of the organisations in AML/CTF are incomplete without incorporating their needs and interactions within the broader context of AML/CTF and crime/terrorism prevention.

Writing in 2002 and referring to growing threat of Al-Qaeda and terrorism John Arquilla (2002) emphasised that "it takes networks to fight networks." According to his logic, an old hierarchical approach to security threats has to be restructured to build an "interconnected strike force of our own". Security studies have followed this trend and inter-organisational, -agency, -sectoral cooperation attracted increasing scholarly attention following the growth of security partnerships between and across public-private sectors (Treverton 2016; Taylor and Russel 2011). Academic theories have evolved around multidimensional layers of analysis aimed to address various levels of "complexities" in cooperation networks (Prezelj 2014). There is no agreement on what factors influence more on inter-organisational networks as type of partnerships can vary in accordance to operational contexts (Perrow 1991). In addition, the debates between constructivists and positivists (Provan and Sydow 2009) have brought to light "external" and "internal" factors (competition, trust, power etc.) of influence through structural analyses (Perrow 1991) or detailed inquiry of managers and personnel within the liaising organisations (Prezelj 2013). While constructivists touch upon an important question of human factor, is the structure that determines a way of cooperation and available opportunities for organisations within a network. Iztok Prezelj (2014, p. 325) writes that "*interagency cooperation* is an effort of state officials from at least two agencies to coordinate their activities or share their sources for the purpose of creating results that a single agency would be unable to achieve". Therefore, "Such cooperation evolves according to the perceived threats, needs, opportunities, and inter-organizational chemistry" (Ibid, p. 327). In this way, in addition to flows of information, it is possible to identify the structural weaknesses within the AML/CTF system.

This research project starts from an assumption that in order to measure the efficiency of intelligence sharing and cooperation, it is necessary to look at a broader network of organisations with specific tasks and needs. A hypothesis is that by outlining the Finnish security environment and AML/CTF structure, it is possible to identify what sort of financial intelligence is generated by the system and required for local police departments as well as flow of information between the organisations. Further, the study will

assess the findings in light of national security strategies to analyse the importance of such information for LEAs in a broader crime/terrorism prevention.

Chapter 2: International, Regional and National AML/CTF efforts

A so-called money trail is not new in criminal investigations and can be traced back to the times of Al-Capone who, by fuelling his illegal alcohol revenues through the cover business of public launderettes, is originally responsible for an emergence of the whole term "money laundering" (Unger 2013). Since then, the approach of "following the money" has rooted deeply in the thinking of law enforcement organisations across the globe and became an integral part of any efforts against organised crime and terrorism. However, international response in this dimension was slow to develop and first measures took place only in the 1990s during the period of rapid globalisation. Aimed to suppress the growing threat of drug trade, international regulations have expanded drastically to include multiple predicate crimes from corruption to terrorism. This chapter will introduce main international and regional organisations as well as national AML/CTF models to create a basis for further analysis of the Finnish structure.

International Organisations

The United Nations

The United Nations is a key organisation in international AML/CTF due to its global outreach, Conventions, and Security Council Resolutions, which are binding for all the member countries. Moreover, the UN has initiated the Global Programme Against Money Laundering operated from the United Nations Office of Drug and Crime that provide training, analysis, assistance, technical information, and expertise for its employees and member states' AML infrastructure (UNODC 2019). On a side of counter-terrorism financing, the UN includes the Counter Terrorism Committee to promote cooperation between the Security Council and member states related to SC resolution 1373 (UNSC 2001), as well as 1267 Committee (UNSC 1999) to identify individuals and entities for freezing their assets.

The UN has adopted three important Conventions that are "Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances" (Vienna Convention), "Convention Against Transnational Organized Crime" (Palermo Convention), and "International Convention for the Suppression of the Financing of Terrorism". Adopted in 1988 and valid from 1990, the Vienna Convention set a requirement of criminalisation the activity of money laundering related to illicit drug trade and limiting the access of criminal money to the banking system (UN 1988). Although not mentioning money laundering directly, the Vienna Convention provides definition of such activity and concentrate on law enforcement and international cooperation issues. The efforts to fight international organised crime were supplemented by

the Palermo Convention in 2000 (UN 2004) that is corresponding to the FATF 40 recommendations and urge to expand criminalisation of money laundering to all serious crimes, establish AML regime, promote national and international cooperation, and consider the establishment of financial intelligence units. Finally, adopted in 1999, the third convention for the suppression of the financing of terrorism (UN 1999) requires criminalising terrorism, organisations and acts with a particular attention to punish any person that aim to provide or collect funds for any of the acts of terrorism. In 2005 entered in force the UN "Convention Against Corruption" (UN 2004) but, with an exception of more detailed attention to the specific predicate crime, it is generally following the lines of the Palermo Convention.

However, in order to become a national law, the UN conventions have to be signed, ratified and implemented by the UN member country what leaves some space for political manoeuvres and limit the scope of international AML/CTF. Therefore, within the hierarchy of the UN, the Security Council has a power to issue resolutions that have to be implemented by all the members. While there are no resolutions on money laundering, the Security Council has taken steps in CTF through Resolutions 1373 (UNSC 2001) and 1267 (UNSC 1999). Including some elements form the Convention for the Suppression of the Financing of Terrorism, Resolution 1373 obliges states to deny and prohibit all forms of support and assistance to terrorist groups, criminalise terrorist financing, and freeze funds, assets, or other resources directed for terrorism. In addition, Resolution requires the UN members to refrain from providing provision of safe heaven or support for terrorists on their side. Most importantly, Resolution 1373 has established the Counter Terrorism Committee (CTC) that is aimed to monitor the performance of the global capacity building against terrorist activity. However, the CTC has no punitive powers and rely on self-evaluation reports coming from the member states themselves.

More precise and targeted actions were set in Resolution 1267 that was aimed against the Taliban and created the "Sanctions Committee" (1267 Committee) to upkeep the list of designated persons and entities (UNSC 2019). After 1999, the responsibilities of the 1267 Committee have grown to cover the activities of Al-Qaeda (Resolution 1333) and obviously ISIL/ISIS in 2015(resolution 2253). Eventually, in 2011, the 1267 Committee was split in two separate groups for AL-Qaeda (and later ISIL) and Taliban (Resolutions 1988 and 1989). Nevertheless, the monitoring teams are concentrated on the main international terrorist movements and have no instruments against other terrorist entities or individuals. Therefore, national states still play a key role in international counter terrorism as for example in case of returning foreign fighters addressed in Resolution 2178 (UNSC 2014).

Financial Action Task Force

The Financial Action Task Force is an intergovernmental body that was established in 1989 by the G7 countries and it aims to "to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system" (FATF 2019e). Therefore, based in Paris in the same premises with OECD, FATF has a responsibility to monitor the implementation of AML/CTF measures among its members, promote FATF standards globally, and report on changing laundering trends. FATF has also established cooperation with similar FATF-style regional bodies and all the organisations that include "a specific anti-money laundering mission or function" in addition to their other tasks and objectives (FATF 2019f). At the moment, FATF includes 37 countries and 2 regional organisations as its members.

FATF has developed 40 recommendations for a comprehensive AML network that is applicable to all the countries around the globe and after 2001 FATF has expanded its reach to CTF through 9 special recommendations (FATF 2019d). As a result, FATF recommendations are seen as a universal international standard for anti-money laundering and are expected to be implemented by every country seeking to obtain international recognition as a reliable actor in AML/CTF. Due to the constantly changing laundering tactics, the recommendations have been revised in 1996, 2001, 2003 and 2012 to incorporate best national practices to the international level. In short, FATF recommendations urge countries to:

1. Develop AML/CTF in accordance to national risks (risk-based approach).

2. Criminalise money laundering and terrorist financing with legislative measures to freeze, seize and confiscate any criminal related property or assets.

3. Set a framework for national cooperation and coordination with appropriate supervision and mechanisms for exchange of information on policy and operational level.

4. Oblige financial institutions to create customer due diligence programs and record keeping for potential investigations as well as report suspicious transactions to FIUs.

5. Create a set of appropriate sanctions for punitive actions against individuals and legal entities related to ML/TF.

6. Establish financial intelligence unit and competent law enforcement and investigative authorities.

7. Promote international cooperation.

8. Monitor national development in money laundering and terrorist financing methods.

9. Follow and implement the requirements set in the UN Conventions and Resolutions that were mentioned above (not a separate recommendation but is mentioned throughout the text).

Despite the fact that FATF recommendations do not have power of law, FATF has developed a capability to pressure countries in case of non-compliance. If any of FATF members refuses to go through or provide information for a two-stage evaluation process (self-evaluation and mutual evaluations), FATF can advise financial institutions to pay special attention to its business transactions with this country or any related individual and organisation. Consequently, these actions will have negative impact on national banking and business services and in worst case scenario a non-compliant country will be suspended from the FATF itself.

Nevertheless, FATF's reach goes beyond its membership and include progress monitoring in other countries and territories. The assessment is done through gathering all the available relevant material such as laws, regulations, and evaluation reports that is then compared to 25 criteria coming from 40 recommendations (FATF 2007). Contrary to the FATF members, non-compliant countries face much harsher consequences with gradual process of escalation measures (Ibid). First, as a warning step, FATF add a country to the publicly available "list of non-cooperative countries and territories" (FATF 2019g) and require special attention from financial institutions. Further actions may lead to enhanced customer identification and stringer requirements for business ties, including systematic reporting to FIUs as every transaction is seen as suspicious. Moreover, FATF can warn non-profit sector about the ML/TF risks in business with the country and even terminate all the financial transactions coming from the FATF member states.

The Egmont Group of Financial Intelligence Units

Nowadays, after 30 years from the first international actions in AML/CTF, financial intelligence units are deeply integrated in almost every national security structure and provide a basis for intelligence sharing between financial institutions and law enforcement agencies. In addition, FIUs conduct various analyses and reports on statistics and laundering methods for other government organisations for various purposes.

Therefore, an FIU "serves as a national centre for the receipt and analysis of: (a) suspicious transaction reports; and (b) other information relevant to money laundering, associated predicate offences and financing of terrorism, and for the dissemination of the results of that analysis" (Egmont Group 2019a). However, organised crime, terrorism, and consequently ML/TF are widely spread on a global scale and in this way require extended international cooperation between states and competent authorities.

Financial intelligence units are not an exception and in 1995 a group of 20 FIUs established the platform for cooperation called the Egmont Group that brings together the heads of units to work on promotion and coordination of national AML programs and initiatives (Egmont Group, 2019b). In addition, including 164 FIUs at the moment, the Egmont Group is a wide network for secure exchange of expertise and financial intelligence through its yearly plenary meetings, working groups, and secure website that is developed exclusively for the use of FIUs (Ibid). The Egmont Group follows the development and implementation of international AML/CTF standards as well as provides publicly available material on ML cases, methods or even operational issues (Egmont Group 2019c). However, it remains unclear to what extent the Egmont Group has operational value as FIUs have direct channels for intelligence sharing between each other and the Egmont Group has no sanctions against non-cooperative jurisdictions. Therefore, group's main outcomes remain on the strategic and policy levels.

Other Organisations

Anti-money laundering and counter terrorism financing are not limited to the previously discussed organisations and one way or another are spread across multiple international institutions in accordance to their respective fields and responsibilities. These include law enforcement, supervision, banking, insurance, customs, and other dimensions that can be penetrated by or related to illegal activities. Taking into consideration the limited scope of this research, a list of FATF liaising organisations (excluding FATF-style regional bodies and organisations introduced above) is added below to provide a rough outline of international AML/CTF network (FATF 2019f):

- African Development Bank
- Anti-Money Laundering Liaison Committee of the Franc Zone (CLAB)
- Asia Development Bank
- Basel Committee of Banking Supervision (BCBS)
- Camden Asset Recovery Inter-Agency Network (CARIN)
- European Bank for Reconstruction and Development
- European Central Bank (ECB)

- Eurojust
- Europol
- Group of International Finance Centre Supervisors (GIFCS)
- Inter-American Development Bank (IDB)
- International Association of Insurance Supervisors (IAIS)
- International Monetary Fund (IMF)
- International Organization of Securities Commissions (IOSCO)
- Interpol
- Organization of American States/Inter-American Committee Against Terrorism (OAS/CICTE)
- Organization of American States/Inter-American Drug Abuse Control Commission (OAS/CICAD)
- Organization for Economic Co-operation and Development (OECD)
- Organization for Security and Co-operation in Europe (OSCE)
- World Bank
- World Customs Organization (WCO)

Regional Organisations and Groups

<u>The European Union and MONEYVAL</u>

International platforms for cooperation bring together differing national priorities that can undermine the dialogue between the countries and slow down or even terminate the implementation of working mechanisms be it in conflict, crime, or terrorist prevention. The current settings of the United Nations with the veto powers and disagreements between the Security Council's permanent members are a notable example of complicated processes of international politics and policy formulation. Moreover, the UN powers of sanctions against the international "outlaws" have demonstrated limited scope of success and partially selective approach to the world crises (Habib 2015), not to mention "minor" issues of implementation of recommended AML/CTF standards. Therefore, international AML/CTF efforts require additional channels and frameworks to reach the national level and the desired operationability. Although FATF has more effective tools of "shaming and blaming", its resources are not sufficient to upkeep the role of global supervisor as it is in case with the mutual evaluation process that take place only once in 4-8 years.

In such complex international environment and lack of proper coercive instruments, regional formations took an additional responsibility to promote AML/CTF in their respective regions and states. This development was particularly visible in the European Union where free movement of goods, services, capital and persons brought a need for a stronger intervention to prevent a criminal abuse of the system. During the time period from 1991 and up to this day, the EU has issued 5 money laundering directives and established a permanent monitoring body of the Council of Europe – MONEYVAL. These steps are aligning with the UN and FATF requirements but have more specific nuances related to the reach and interpretation of customer due diligence, reporting, and predicate crimes.

First EU Directive 91/308/EEC "on prevention of the use of the financial system for the purpose of money laundering" (EU 1991) gives a definition of money laundering activity but most impotently it outlines the responsibilities, tasks and particular guidelines for financial institutions and "competent authorities" of the member states. The document set a threshold of 15000€ (ECU back then) and requires its members to ensure that credit and financial institutions take proactive steps in reporting suspicious activities above the threshold with appropriate internal controls to avoid carrying out suspicious transactions. However, even transactions below the threshold have to be reported in case if they can be related to money laundering. In this way, the directive brings together the knowledge in possession of the private sector and expertise of government officials to establish a system of filters that would collect the arriving leads and filter them for law enforcement investigations. In order to monitor the transportation of the directive to national law, promote dialogue and gather feedback from national state, the EU created a contact committee with the appointed persons from the member states and committee itself.

Soon after the introduction of AML tools, criminals have learned to avoid the threshold of suspicious transactions and shifted their attention away from the heavily regulated financial sectors (mostly banks) towards low-value operations and less regulated intermediates (FATF 2018). This development was then reflected in the second directive 2001/97/EC (EU 2001) that is, similarly to all the following directives, an amendment to the first document with the intention to close the gaps coming from practical experience. The second document adopts the approach of the UN Vienna Convention to include the similar types of serious predicate crimes but also expands its scope to fraud, corruption, participation in the activities of criminal organisations, and any "offence which may generate substantial proceeds and which is punishable by a severe sentence of imprisonment in accordance with the penal law of the Member State". In terms of reporting requirements, the European Commission decided to include a list of professions such as auditors, real estate agents, notaries and dealers of high-value goods which, in additional to traditional financial institutions, could serve the interests of criminal actors. The most interesting step was to include legal professionals to the reporting processes what sparked the debates

around the client-attorney privilege and has various legal outcomes in different member states (Utrecht University 2013, pp. 76-79).

Nevertheless, starting from 2003, the international AML/CTF has slowly shifted from the rule-based to the risk-based approach due to highly unpredictable and complicated nature of illicit flows. In this context, contrary to the previous attempts to set the clear and unified criteria for effective counter-measures and information gathering, the risk-based approach emphasises the importance of understanding the areas of high, medium, and low risk in various spheres of countries', state authorities' and private sector's field of responsibilities. According to this logic, the identification of risks should determine the levels of scrutiny of AML/CTF programmes depending on the particular ML methods and threats to a state or an organisation. Therefore, the third EU Directive 2005/60/EC (EU 2005) is an attempt to make customer due diligence (CDD) more effective in gathering relevant information such as on "politically exposed persons" to address the most pressuring threats. The directive provides the guidelines on simplified and enhanced CDD procedures with a special attention on beneficial ownership that goes beyond the previous requirements of identification of middlemen and managers. However, in this document, the list of predicate crimes has been expanded further to include financing of terrorism as a serious predicate crime adopted from the Framework Decision 2001/500/JHA (EU 2001). In addition, following the UN Resolutions 1373 and 1267, the EU has implemented its own practise of listing terrorist persons and entities (EC 2019).

The most recent actions in the EU AML/CTF are the fourth directive 2015/849 (EU 2015) and the fifth directive 2018/843 (EU 2018) that has to be implemented by 10 January 2020. Both of the documents address the issues of national and international cooperation, adjust the risk-based approach with clarification in cross-border situations, and include the emergence of new technologies such as virtual currencies and pre-paid cards. In this regard, the directives enhance the powers of national FIUs and their access to broader information, set a criteria for the assessment of high-risk third countries, as well as require the established of publicly available registers on companies, trust and other legal arrangements. It is worth to mention that all the directives were followed by intensified discussions around the impacts of the AML/CTF system related to data protection, legal outcomes and general burden to the private sector (for example Harvey 2004). Therefore, similarly to FATF and UN, the EU directives have left a considerable space for national adjustments in the implementations of its requirements.

Finally, starting from 1997, the EU includes "The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism" (MONEYVAL) that is responsible for assessment, monitoring and providing recommendations to national authorities related to international

AML/CTF standard (Council of Europe 2019). In addition, the Committee provides technical assistance, training, and annual reports to raise the awareness and contribute to the global fight against money laundering and the financing of terrorism. Therefore, MONEYVAL is FATF-style Regional Body that concentrate on the jurisdictions of the European Council that are not members of FATF or voluntarily agree to participate in additional assessment regardless of their FATF membership.

FATF-style Regional Bodies

FATF-style Regional Bodies are voluntary and cooperative organisations that follow the steps of the Financial Action Task Force in monitoring and research procedures. These organisations are formatted on the regional basis and membership is open to any country from the same geographic area that is willing to accept the working principles of the bodies. In this way, the international AML/CTF standards are getting a supplementary global outreach and most importantly typology reports on ML/TF methods related to the specific nature of every region. The Regional Bodies can also issue their own additional recommendations as in case of CFATF with the 19 "Aruba Recommendations" (IMOLIN 2019) from the perspective of the Caribbean region. In addition to MONEYVAL, there are eight regional organisations that are listed below:

1. Asia/Pacific Group on Money Laundering (APG)
2. Caribbean Financial Action Task Force (CFATF)
3. Eurasian Group (EAG)
4. Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG)
5. Financial Action Task Force of Latin America (GAFILAT) (formerly known as Financial Action Task Force on Money Laundering in South America (GAFISUD)
6. Inter Governmental Action Group against Money Laundering in West Africa (GIABA)
7. Middle East and North Africa Financial Action Task Force (MENAFATF)
8. Task Force on Money Laundering in Central Africa (GABAC)

National AML/CTF Models

As it becomes evident from the previous parts of this chapter, the international development in AML/CTF has seen a significant improvement to address constantly changing criminal behaviour. All the international and regional organisations are in a good balance with each other and promote the implementation of unified models for effective cooperation, prevention, research, supervision, enforcement and other aspects of problematic dimension of money laundering and terrorist financing.

However, regardless of the comprehensive international tools and efforts in this field, the question of illicit flows is far from being resolved and there is no evidence of decline in ML/TF. While part of the explanation lays in the international context itself and in the methods of measurement (Lavi et al. 2018), the other side of the coin can be found in varying national regimes with the complexities and incapability between them. This means that, during the transition of AML/CTF laws and requirements to national security structures, states have adopted those measures in accordance to their legal circumstances and priorities.

Under careful analysis, these differences form considerable challenges of various extent for an uninterrupted prevention and prosecution of ML/TF. In the ECOLEF project (Utrecht University 2013) on the legal and economic effectiveness of the national AML/CTF structures within the EU borders it is well presented that the member states have applied different solutions in regard to legal privilege, reporting procedures, legal definitions and supervising authorities. In this way, one country might exempt auditors from reporting duties and prosecute money laundering related only to "external" launderers (a person who assists criminal actors in ML) while another takes a broader approach and chase self-launderers (same person who also committed a predicate crime) inclusively. In addition, customer due diligence programmes can be implemented only to major financial institutions with no significant effort to include other financial service providers into the reporting framework. Therefore, based on these specific decisions, an AML/CTF model provides different intelligence products and leads to various outcomes in crime prevention. Moreover, international cooperation can be undermined by inability of a state to react and receive information in a timely matter for effective identification and seizure of dirty money. In this regard, one of the most important development in the national AML/CTF setting is the position of a financial intelligence unit within the national security structure.

According to the overview done by the International Monetary Fund (2004), there are roughly four types of financial intelligence units which have different objectives, responsibilities and access to databases. At the beginning of the international AML/CTF there was no single definition of "competent authorities" for combating money laundering and states were forced to establish new organisations or adjust the existing institutions with new units. Only in 2003, as for example in the revised FATF recommendations and the Palermo Convention, the established authorities received the name of financial intelligence unit and more clarified guidelines regarding their activity. Nevertheless, national variations of FIUs required a formulation of coordinative actions and strategies to promote a unified approach in counter-measures what partially falls into the responsibilities of the Egmont Group. At the same time, each of the type of "judicial", "law enforcement", "administrative" and "hybrid" financial intelligence units determine the priorities of national model and type of intelligence that is circulating within the official channels. By

looking at the flows of information and type of intelligence in possession of FIU, it is possible to identify to what role does the FIU play in the system and to what extent it is able to satisfy the intelligence needs of law enforcement and other organisations.

Judicial model of FIU set the unit as a part of the prosecutor's office and brings into play judiciary powers for effective seizing of funds and further actions that require immediate response. The Judicial FIU can cross-check the received leads with judicial information and provide more polished intelligence for investigative and prosecuting authorities that is then turning into evidence in court cases. In this setting, the FIU is well aware of the work of the prosecutor's office and needs less feedback from law enforcement agencies on the type of information and quality of disseminated information. The judicial FIU is most common for the countries where judicial system can direct and supervise criminal investigations and investigatory bodies what also put more pressure on financial institutions to follow the reporting procedures. Other benefits of this model are the higher degree of autonomy from political interference and minimal layers of organisations between the reporting entities and investigative/prosecuting authorities (IMF 2004, p.16). On the other hand, while having the access to judicial information, this model of FIU is relatively distant from regulatorily databases and criminal intelligence in the possession of the law enforcement agencies. In addition, judicial FIU share similar disadvantages with law enforcement FIU that are, for example, prioritising investigative measures over prevention and obstacle of launching formal investigations to access financial information of an organisation (Ibid).

Some countries have decided to establish their FIUs as part of law enforcement agencies with an emphasis on enforcement aspect and appropriate powers within the existing legal and administrative framework. Therefore, law enforcement FIUs may have similar powers to judicial type FIU in terms of seizure and freezing of assets as well as conducting interrogations and searches. Moreover, LEA type FIUs have a direct access to criminal intelligence and are closer to the special units within police forces that concentrate on financial crimes and terrorism, what brings additional sharing of expertise and knowledge in coordinated manner. Simultaneously, law enforcement agencies have a direct access to FIU's information what improves its usefulness and precision in criminal and intelligence investigations. However, the biggest disadvantage of LEA and also judicial type FIUs is possible reluctancy of financial institutions to disclose sand share information with such agencies. IMF (Ibid p. 14) emphasises that "law-enforcement agencies are not a natural interlocutor for financial institutions; mutual trust must be established, which may take some time, and law-enforcement agencies may lack the financial expertise required to carry out such a dialogue". Also, "reporting institutions may be reluctant to disclose

information to law enforcement if they know it could be used in the investigation of any crime (not just money laundering and the financing of terrorism)" (Ibid).

In order to avoid the disadvantages and promote more natural cooperation between the financial sector and national authorities, certain states have established an administrative type FIUs that are under supervision of an administration or an agency other than law enforcement. Conclusively, "The main rationale for such an arrangement is to establish a "buffer" between the financial sector (and, more generally, entities and professionals subject to reporting obligations) and the law-enforcement authorities in charge of financial crime investigations and prosecutions" (Ibid, p. 10). In this particular setting, an FIU might be a part of a central bank or fall under the framework of ministry of finance and, therefore, establishing its access to regulatory databases. At the same time, an administrative FIU is a purely passive player within the network and has relatively weak access to criminal records, intelligence information and judicial sources. Deleanu (2013, p. 466) points out that "from an intelligence gathering point of view, in this system, a large amount of information from criminal sources circumvents the screening of the FIU. Furthermore, there is little interaction between the prosecution and the FIU, and hence the end- user might lose sight of what the FIU is or should be doing". Moreover, a significant disadvantage of an administrative type FIU is the lack of powers of law enforcement and judicial authorities to act on urgency cases in seizure and confiscation of assets.

Last type of FIU has no particular categorisations and it is officially labelled as a "hybrid" model that incorporates various characteristics from all the previously mentioned models. This model is an attempt to effectively implement working features of all the other models to find a flexible solution for counter-measures. Financial intelligence units of hybrid nature can be a result of merged
organisations, personnel with powers from other agencies, or combination of crossing powers and data access from parallel jurisdictions (police, custom etc.).

Chapter 3: Finnish Security Environment and AML/CTF Structure

Security environment

Current AML/CTF standards are predominantly emphasizing the so-called "risk-based" approach that intends to equip countries and reporting entities with an adoptable thinking to the challenges coming from ML/TF. For example, FATF and the most recent EU directives require its member states to conduct national risk assessments in order to identify, assess, and understand the national risks on a regular basis, and apply their counter-measures accordingly. This form of thinking is different from the "ruled-based" philosophy that aims to pre-determine the applicable measures and simultaneously limit the space for interpretation and different variations of AML/CTF procedures within the reporting entities as well as national authorities (Costanzo 2013, pp. 350-352). Therefore, the "rule-based" approach is also based on a general evaluation of risks but tries to incorporate a unified set of rules, which eventually will be useful in all the cases of money laundering and terrorist financing. In this way, the responsibility of preventive measures lay solely on governments while financial institutions have to carefully follow the established framework and guidelines. The situation is different with the acknowledgment of unpredictable and fluid nature of criminal behaviour what makes it impossible to calculate all the ML/TF variations in different fields and jurisdictions. Conclusively, the "risk-based" perspective is an attempt to share the tasks between private and public sectors as well as to maximise efficiency of practical experience of financial institutions and government officials in their respective spheres of influence.

In practice, the "risk-based" logic is particularly useful in forcing financial and credit institutions to develop a deeper knowledge regarding relevant markets, services, products, customers, and other aspects that could prevent the illegal activity and actors in cleaning their money. Accordingly, this requirement creates an additional filter for information going to a financial intelligence unit and other authorities. At the same time, similarly to the states on the international level, private sector professionals can cumulate their knowledge of best practises in form of general overviews and specific guidelines for lawyers (Suomen Asianajajaliitto 2017), real-estate agents (Kiinteistönvälitysalan keskusliitto 2018), auditors (Suomen Tilintarkastajat 2017) and other lines of work. Therefore, shared responsibilities and application of relevant expertise increase the precision of national AML/CTF structure on strategic, operational and tactical levels. This means, for example, that: 1. suspicious transaction reports will include more relevant information and require less time for investigations, 2. financial institutions will be better equipped with tools to identify illicit behaviour, 3. financial information will be more usable for national and international cooperation, 4. supervision will become more efficient, and 5. relevant authorities can exercise their powers in more rapid way to prevent the illicit flows of funds. On the other hand, to adjust

their scarce resources and regulations to the most vulnerable sectors for ML/TF, national authorities have to upkeep a much broader situational awareness of methods and actors in their unique security environments.

By identifying criminal actors and methods, states can close the gaps in AML/CTF models and increase its capability in prevention and investigation of criminal cases. Coming to the Finnish security landscape, it is identifiably that over the years its development has been influenced by the geographic location, EU membership and lack of internal borders, increased volume of immigration, technological progress, and domestic transformation of the criminal underworld. In the recent FATF evaluation report (2019a) it is stated that "Given its geographical location, Finland is a major European gateway to and from non-European countries, and strong business and trade relationships have developed between Finland and Russia, as well as with neighbouring Baltic States and other Nordic countries. This geographic proximity supports the development of commercial routes, including trade routes in illicit flows of goods and funds". The dark side of trade and business can have many beneficiaries but most dangerously it quickly attracts all types of organised criminal groups which aim to increase its influence, hide the illegal funds and multiply their illegal revenue through the legal sources. Therefore, it is important to understand the features of these groups, which are originally the main target for the AML/CTF regimes and law enforcement agencies.

According to the Finnish police "Handbook on Prevention of Organised Crime" (Suomen Poliisi 2019a), there are approximately 90 organised criminal groups operating in the country, from which about 70 are the so-called "symbolic" gangs that have clear identifiers of their criminal orientation. The biggest majority of those groups are the violent motorcycle gangs with a traditional scope of criminal activity of drug trade, racketeering, arms trade and human trafficking (Salminen and Suomala 2018, pp. 21-24). It is estimated by the police that the rapid growth of motorcycle gangs from the four major groups in the beginning of the 2000s up to almost 70 in 2019 is a clear indicator of the growing criminal threat. While small groups have limited power of influence and access to resources, part of the Finnish "criminal bikers" belong to the wider international and regional networks such as "Hell's Angels", "Bandidos" and "Satudarah". Moreover, due to the tight criminal market there is an evidence of growing cooperation among various groups of international and Finnish origin (Iltalehti 2010), as well as additional emergence of new formations such as Russian "Night Wolves" (Iltalehti 2019). Therefore, the fundamental members of the Finnish underworld are growing their capabilities over the borders and follow the trends of international crime networking developments.

Furthermore, growing globalisation and high volume of immigration have brought new opportunities for the local gangs with an easier access to the criminal markets and expertise within the EU but also wider connections to the third countries. Predominantly Finnish gangs have started to actively recruit new members with foreign origin from the immigrant and refugee communities (Iltalehti 2018), who have specific language and regional knowledge to establish relationships with criminal actors in their home countries. Also, members with foreign origin can have access to immigrant communities living in other European countries to gain support in transit of arms, drugs and humans. Such examples can be already found in Sweden with the Balkan connections and refugees from the region (Huhtamäki 2019) what is also emerging in Finland through the crawling influence of Albanian organised crime (Suomen Poliisi 2019a, pp. 19-21). On the other hand, due to the enlargement of the Schengen zone, Finnish security environment has witnessed an influx of ethnic gangs and criminal elements from Poland, Romania, Bulgaria, the Baltic States, and the Post-Soviet space more widely. In this way, new actors have adopted to the available opportunities and specific crimes as in case of African gangs and fraud, drug and human trade, as well as robbery and itinerant Georgian groups (Ibid). As a result, rapid internationalisation of the criminal underworld has brought to light previously unknown forms of criminal elements of "thieves-in-law" and other influential financial and power players.

Contrary to organised crime, terrorist activity and its financing have different form and objectives. Although crime-terror connection brings additional income to terrorist actors, legal sources of business and financial transactions can be equally utilised for terrorist acts in purpose to spread fear, chaos and violence in a targeted state. So far Finland has avoided major terrorist attacks with an exemption of "Turku terrorist assault" in 2017 conducted by an asylum-seeker of a Moroccan descent which left 2 people dead and 8 injured (Rimpiläinen and Mansikkamäki 2017). Nevertheless, the Finnish Security Intelligence Service (the SIS) evaluates that the level of terrorist threat to national security is now "increased", and there is a growing influence of radical Islamic ideology due to the propaganda efforts from the inside and abroad (SUPO 2018). Other potential threats of an already formatted "jihadi-underworld "(Paananen 2019) are described to be in form of "lonely wolves", "returning and other foreign fighters", "influential inciters" or "significant financial supporters" (SUPO 2018, pp. 28-29). The most worrying development is the expanding "surveillance" list of individuals with terrorist connections which now includes 370 persons (Ibid. pp. 32-33) compared to only 70 in 2012 (SUPO 2017). Therefore, terrorist activity poses an additional challenge to the AML/CTF efforts and national security structure in general. Particular issue is to identify case of terrorist financing in hawala systems, charities, and misuse of social benefits, for example (Malkki and Saarinen 2019, pp. 91-93).

The identification of criminal/terrorist actors and dominating predicate crimes in national security environment is particularly important for the law enforcement and intelligence agencies. However, from a perspective of a strategic analysis for more effective AML/CTF guidance, it is equally decisive to identify the methods of moving toxic money and, therefore, vulnerabilities in the financial system. In 2015, conducted by the Police University College in cooperation with national authorities and private sector representatives, Finnish government issued a national risk assessment of money laundering and terrorist financing (Jukarainen and Muttilainen 2015). The document introduces main methods of ML/TF and vulnerabilities that require special attention in Finland. This range of weaknesses includes "investment in real estate", "cash smuggling", "cover businesses", "digital payment services", "online fundraising" and "client asset management" (Ibid, pp. 105-107). These findings are based on the practical experience and estimates of professionals coming from all levels of the Finnish AML/CTF and related financial industries that are then put in the context of international developments in the field.

Starting from the real-estate sector, the national threat assessment outlines that, in light of consequences to national economy and society, this sector is particularly important for AML/CTF. The lack of appropriate supervision over the sector as well as insufficient means to verify the origins of funds coming from foreign investors pose a gap for the preventive measures. Real estate agents emphasize that it is difficult to remain confidentiality of reporting persons in case of suspicious transactions. In additional, only few real-estate agents have up-to-date and comprehensive guidelines of ML with no available instructions on terrorist financing. Although not mentioned in the assessment itself, there are few examples where arguably poorly regulated real-estate sector helped the illicit actors from neighbouring countries to move their illegal funds coming from crime and corruption (Paunonen 2018). Similar difficulties with proper regulations can be found more generally in client asset management where accounting principles are not properly defined by law and are arguably one of the most common methods of ML/TF. Moreover, an open competition in trade of securities and bonds complicate the information gathering especially from abroad.

The usual international menaces of "cash smuggling" (Cassara & Jorisch 2010, pp. 39-55) and "cover businesses" (Bernstein 2017) are also present in Finland with specific challenges for border control and financial crime prevention. As part of the assessment, the Finnish border control has pointed out the difficulties in prevention of "cash smuggling" within the EU internal borders and lack of means to identify cash for terrorist purposes. While organised criminal groups can aim to smuggle large amounts of banknotes, terrorists and their supporters may rely on significantly lower amounts without even reaching the reporting threshold (Cassara & Jorisch 2010, pp. 39-55). Moreover, the Finnish financial intelligence unit and border guards have powers to seize suspicious fund for only for ten days (act 445/2017) for

further investigation. Therefore, without identified crime, cash recipient or open criminal investigation in the country of generated funds, the Finnish authorities have no means to prevent cash from entering the country and the Schengen zone. At the same time, "cover businesses" or "shell corporations" are another form to disguise criminal origin of funds and this method is especially applicable in the dimensions of "grey economy" for tax evasion and avoidance of other statutory payments (Bernstein 2017). In the Finnish context, "grey economy" and related financial crimes are seen as the dominating form of ML/TF with particular influence in businesses of construction and logistics (Jukarainen and Muttilainen 2015, pp. 105-107).

Finally, the advancement of payment and communication technologies has opened a window to more sophisticated and safe methods of criminal operations beyond the reach of regulatory powers. Those include "virtual currencies" (Hunt 2011), fraud schemes (source), terrorist fundraising (Cassara & Jorisch 2010, pp. 137-157), and of course traditional crimes of various types (Goodman 2015). The Finnish risk assessment concentrate its attention on "online fundraising" and "online payment services" that briefly include gambling, virtual currencies, mobile payments and other online financial services (Jukarainen and Muttilainen 2015, pp. 105-107). Therefore, the document points out the emerging difficulties of that time which would be later addressed in various national documents related to broader use of NGOs for terrorist financing (Arpajaishallinto 2019) and other issues.

In conclusion, as it is visible from the introduction above, Finnish security environment incorporates various illicit actors with connections to the underworld and terrorist networks. Moreover, available opportunities and vulnerabilities on the national and international levels provide these actors with sophisticated methods to move money across and beyond national jurisdictions and financial sectors. FATF report (2019a) concludes that, based on the security context, the dominating ML/TF crimes are coming from "grey economy" (e.g. financial crimes), drug trade frauds of various kind and terrorist sympathisers. Therefore, the most pressuring issues that have to be addressed are business relationships with neighbouring countries, grey economy and tax evasion, supervisory framework, transport of cash, hawala institutions and NGOs, and real-estate, gambling, and precious metal and stone sector (?). The analysis of this research mostly corresponds to the findings of FATF but with an exception that other predicate crimes of human and arms trade and domestic organised groups should be equally addressed in AML/CTF to upkeep the crime prevention in light of growing organised crime. In addition, as part of the country assessment, FATF has used additional sources from "international organisations" that were not identified and, therefore, could not be verified as in case of precious metal and stone sector. Nevertheless, we agree that the national AML/CTF model have to be properly equipped to supplement the efforts of law enforcement and intelligence agencies in crime/terror prevention, identification, and disruption.

Finnish AML/CTF Model

In general, Finnish AML/CTF model is corresponding to the international requirements and follow the established framework of the organisations introduced in chapter 2. The major guiding organisations are the United Nations and its Security Council, Financial Action Task Force, and the informal organisation for national financial intelligence units - the Egmont Group. In addition, Finland has signed, ratified and implemented the Vienna "Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances "in 1994, followed the same path with the "Convention Against Transnational Organized Crime" in 2004, as well as adopted the conventions on suppression of terrorism in 2002, and convention on corruption in 2006. Finland has implemented one of the most extensive AML/CTF models in accordance to 40 recommendations and the EU directives which aim to cover a broad range of reporting entities and provide detailed guidance on "risk-based" approach for the private sector professionals (KRP 2012). Therefore, Finnish AML/CTF structure has multiple tools for international and national cooperation, asset seizure and freezing, wide range of supervising authorities, and analysis of changing trends in money laundering and terrorist financing.

On the national level, the legal principles for the national counter-measures are founded through the criminal law, the "act on Preventing of Money Laundering and Terrorist Financing (444/2017)", the "act on the Freezing of Funds with the View to Combating Terrorism (325/2013)", and the "Act on the Financial Intelligence Unit (445/2017)" (Suomen Poliisi 2019) as well as Criminal Code (39/1889). These legal documents provide definitions of activities related to ML/TF, predicate crimes, reporting obligations and entities, as well as powers of the national authorities and the financial intelligence unit. In this way, according to the Finnish law, money laundering is a punishable crime in case of if an individual "accepts, uses, converts, hands over, moves, transmits, or possesses assets of criminal origin with an intention to benefit itself or assists others to benefit from these funds, cover or hide illegal nature of assets, or help criminals to avoid legal consequences " (own translation from source act 39/1889). Accordingly, terrorist financing is a punishable crime if an individual "either directly or indirectly provides or collects funds with an intention of financing or knowing that these funds will be used for the defined terrorist acts" (own translation from act 39/1889). Terrorist acts are then described in five different categories. However, interesting exception is that in both cases terrorist financing and money laundering charges are not applicable if a person is charged or convicted directly of a predicate crime or terrorist activity. Therefore, self-launderers and terrorist actors will not be prosecuted for ML/TF by the Finnish system.

Coming to the reporting entities and supervision, Finnish law obliges (act 444/2017) to establish reporting procedures and AML/CTF measure to all the organisations and individuals working in the field of (simplified list):

1. credit, finance and investment sectors

2. pawnbroking

3. insurance

4. gambling, casino and betting services

5. real-estate sector

6. accounting and auditing

7. tax advisement

8. legal services

9. sales of goods if transactions happen in cash over the set threshold

10. property management and business services

These fields of reporting entities are then divided between the appropriate supervising authorities in form of

1. Financial Supervisory Authority (financial sector)

2. National Police Board (gambling)

3. the Local Government of Åland (gambling in Åland's jurisdiction)

4. Finnish Chambers of Commerce and Finnish Patent and Registration Office (accounting and auditing)

5. Regional State Administrative Agencies (pawnbroking and property management services)

6. the Finnish Bar Association (legal service)

The supervisory authorities have various powers to enforce AML/CTF requirements in their respective fields as well as to provide, monitor and implement best practises in accordance to changing trends in money laundering and terrorist financing. Therefore, the AML/CTF standards should cover all the main fields of vulnerable sectors and provide relevant information to national authorities. However, the situation is more complicated as it was mentioned in the previous part on security environment.

In practice, the guidelines for reporting entities are done in form of the so-called Customer Due Diligence procedures that go through the general processes of business client relationship. In 2012, the Finnish FIU has released a handbook on "best practises in money laundering prevention" (KRP 2012) and opened the main paragraphs from the related legislation. The handbook outlines the major rules that the reporting

entities have to follow from establishing a relationship with a costumer, during their business transactions, to the terminations of service providing. in that way, it is necessary to confirm a real identity of the customer, a real beneficial ownership behind the legal entity, follow and monitor clients' transaction in order to uncover suspicious changes in behaviour, and keep all the related document available for the national authorities for minimum five years. There are two due diligence procedures that are simplified and enhanced customer due diligence. Before being applied, both of the approaches have to take into consideration all the influential factors such as the level of risk in a country of origin, including sanctions, political situation and corruption. In addition, client background, field of business, owners, size and frequency of transactions, product risk, and other factors should be evaluated for further procedures of CDD. Nevertheless, it is worth to mention that financial institutions and other reporting entities have no access to extensive data of government organisations and have to operate based on the limited available information.

The reporting framework is not only limited to the private sector and includes few government organisations with a particular requirement to pay attention to ML/TF in addition to their other objectives. Those organisations are Finnish Customs, the Border Guard, the Tax Office, the National Administrative Office of Enforcement, and the Office of Bankruptcy Ombudsman. In addition to monitoring requirements, the Finnish Customs and Border Guards have powers to seize suspicious cash transportations up to ten days. The procedure may happen on the request of the leading officers from the financial intelligence unit but at the same time customs, border, and police officials are required to seize all cash transportation over 10000 euros crossing the EU external borders without appropriate documentation (Jukarainen and Muttilainen 2015, p.36). On the other hand, these procedures, monitoring and AML legislation do not apply to the EU internal borders.

Finally, the central authority that receives, analyses and disseminates suspicious financial information is the Finnish financial intelligence unit. In the "Act on the Financial Intelligence Unit" (Act 445/2017) main activities and duties of the unit are described to include (simplified list): 1. ML/TF prevention, disclosure, analysis and bringing for investigation, 2. analysis of suspicious transaction reports and provision of feedback to the reporting entities, 3. cooperation with other national and international authorities as well as reporting entities in ML/TF prevention, an 4. conducting of statistics on the amount of reports, asset freeze orders, cooperation requests and other information. Moreover, as part of the main functions of the FIU, the act established the so-called "money laundering register" that will include relevant financial intelligence in possession of the unit. The register can include all the personal details of the suspected criminal individual and terrorist actor. Therefore, established in 1998 as part of the National Bureau of Investigation the financial intelligence unit partly enjoys the powers of law enforcement

organisation and is an indicator of an investigatory orientation of the Finnish AML/CTF model. The FIU can seize suspicious assets for ten days and investigate reported cases of ML/TF. In case of further investigation and prosecution, the FIU is required to handle its cases to the National Bureau of Investigation, the Local Police Departments or the Security Intelligence Service.

From the perspective of the national security environment, the Finnish AML/CTF model is generally well structured to address the challenges of organised crime, terrorism and ML/TF related predicate crimes that generate a large amount of funds and might affect various sectors of national economy. The issues with neighbouring countries, grey economy and tax evasion, supervisory framework, transport of cash, hawala institutions and NGOs, and real-estate and gambling sectors are not easy to address as its well demonstrated through the international experience (for example EUROPOL 2015). Nevertheless, the Finnish authorities have made progress to improve some elements of the AML/CTF model. Most importantly, the adaptation of the strategic document based on the Finnish Government Resolution "on the prevention of "grey economy" and financial crimes for 2016-2020" (Valtioneuvosto 2016) for guiding the cooperation of authorities in prosecution, investigation, identification, and prevention of financial crimes, but also money laundering as part of this activity. As part of the strategy, it is emphasised the importance of guidance and advisement of supervisory authorities for further improvement the reporting entities. In this regard, Tax office's "Grey Economy Information Unit" produces and disseminate valuable strategic reports on recent developments (Verohallinto 2019). Also, additional guides were published for real-estate (Kiinteistönvälitysalan keskusliitto 2018) and non-government organisations (Arpajaishallinto 2019).

On the other hand, the transport of cash, criminal funds coming from abroad, and hawala institutions are a particular challenge that is to an extent out of reach of national authorities. While the Border Guards continue to monitor the transport of cash over the EU external borders, cash smuggling remains to be the biggest problem in ML/TF that cannot be addressed alone by any country (EUROPOL 2015). Similarly, the identification and filtration of funds coming from abroad is a daunting task that poses a risk of over-regulation and disruption of healthy business transactions (MONEYVAL 2015). Private sector has limited tools and access to information what is especially problematic with states with high corruption and unstable situation. Finally, Hawala money transfer institutions have been on the agenda of the international AML/CTF since the beginning of the "war on terror" (Zakarte 2013) and has no visible results in preventing the constant abuse for terrorist and criminal purposes. Hawalas are trust-based money remittance services where money does not physically leave a country what is a challenge for monitoring actions. In addition, millions of people are using the system to send money to their relatives living in the conflict zones that would potentially be used for terrorist purposes, but cannot be verified

without knowing identities of illicit actors. Therefore, while all the issues are acknowledged, and various solutions are introduced in theory, it remains to be seen what frameworks will be implemented in the future. In this regard, no visible progress has been made by the Finnish authorities.

Financial Intelligence Unit and Intelligence Sharing

International connections of terrorist and criminal actors as well as globally spread infrastructure of finance, trade and business increase the importance of various forms of cooperation between national and international authorities. The forms of cooperation might include technical assistance, sharing of equipment and personnel, and financial support, but at the central role of any combined efforts in crime and terrorism prevention is intelligence sharing. A valuable piece of information can be crucial in identifying illicit actors, criminal investigations and preventive measures of related organisations. Different officials and private sector representatives have various levels of expertise and access to databases that can effectively supplement their effort in achieving mutual objectives. With the expertise of financial intelligence units and its legal powers to obtain information from the reporting entities, law enforcement agencies and AML/CTF organisations receive an important support in form of analyses and reports. Moreover, within the wide network of AML/CTF, based on the provided information private and public organisations can conduct their tasks in more precise way with limited negative impact for licit business or financial activity. However, it should be kept in mind that AML/CTF related organisations have other tasks and priorities including their own sources of information. Therefore, in order to evaluate efficiency of cooperation and relevancy of information it is necessary to identify what sort of and where financial intelligence is going in the system. The FATF report (2019a) provides a comprehensive overview of the FIU gathering, analysing and disseminating functions that will be introduced below.

The Finnish AML/CTF model has established a law-enforcement type financial intelligence unit as part of the National Bureau of Investigation. Therefore, the FIU has a wide access to police databases and criminal intelligence including the information from the local police departments. FATF report outlines that all together the FIU has direct access to:

1. Vehicle and Watercraft Registers
2. Driving licences
3. Passport Register (Finnish passports)
4. Border crossings of persons entering Finland with a visa;
5. Visas granted by Finland to foreign nationalities
6. Land Information System
7. Register of Aliens by Finnish Immigration Service

8. Criminal Investigation Database (Police, Customs, Border Guard)

9. Criminal intelligence database (Police, Border Guard)

10. Schengen Information System (SIS II)

11. Europol SIENA and EIS

12. Interpol I24/7

13. Database on International Information Exchange (i.e. incoming/outgoing requests)

The access to databases is then supported by the reports coming from the reporting entities from private and public sectors. Moreover, according to the Act on the Financial Intelligence Unit (act 445/2017), for the purposes of prevention and investigation of ML/TF cases the FIU can request all the necessary information and documents from individuals, organisations and government officials, regardless of the "confidential" restrictions set in other legislative documents. In this way, the FIU is granted with a strategic position to comprehensively supervise the ML/TF security landscape.
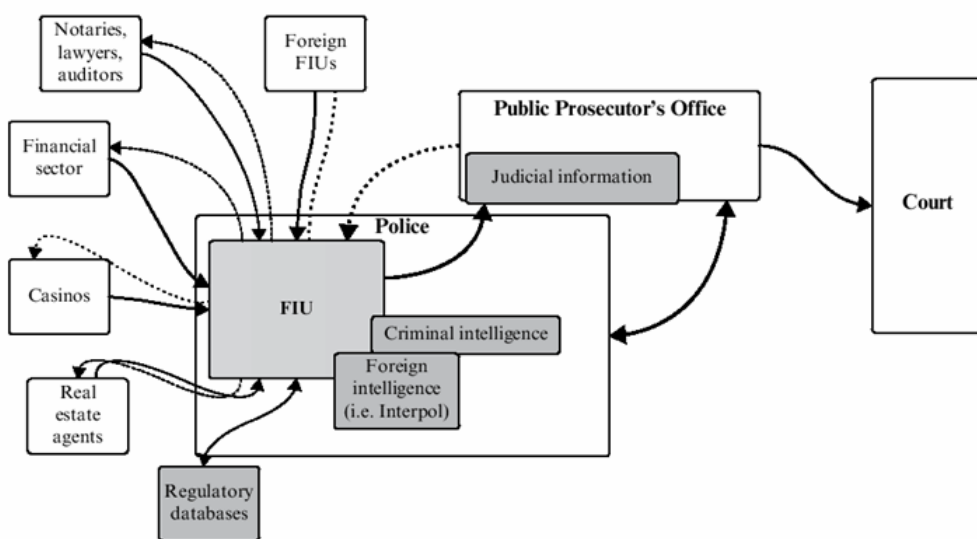
Figure 1: the law enforcement FIU (Deleanu 2013, p.467).

The information from the reporting entities comes in forms of "suspicious transaction" (STR), "threshold" and "compliance" reports including also "cross-border cash" declarations (FATF 2019a, pp. 50-59). Suspicious transaction and threshold reports are mostly filled by the private sector reporting organisations, but previously mentioned national authorities (see previous part) are also obliged to report on suspicious cases in their jurisdictions. As the main source of financial intelligence, STRs include a list of 34 indicators which help to narrow the scope of analysis to relevant information and filter out unnecessary flow of "overreporting". The "threshold" report provides technical information about the

transactions reaching an individually set threshold for every field and organisation (Ibid). The amount might be set by authorities, but it is mostly identified by the internal risk analysis within the institutions themselves. In this way, gathered information is not comparable to STRs and aim to provide additional source of information. Cross-border cash declarations are filled by the Finnish Customs and include transports of cash over 10000€ entering or leaving the EU borders (Ibid). Finally, compliance reports are coming from the "grey economy information unit" (GEIU) and provide intelligence information on financial crimes and tax evasion. The access to all the reports between the authorities varies in accordance to their field of responsibility but part of this information is available to the police departments as well.

In terms of analysis, the arriving information is categorised by its type and relevancy either to update the databases or investigate on suspicious behaviour. Arriving STRs are usually analysed individually by one of the officers working in the FIU and thus information is cross-checked with all the available source with the help of enhanced IT programs (Ibid). In case if an STR matches with one of the databases and/or GEIU information, the FIU applies an "enhanced" analysis of transaction to link the subjects, transactions and potential crime activity. Further actions might include escalation of investigation in form of a "case" by the approval of the commanding officer and prioritised in accordance to the list of ML/TF risk profile. The risk profiles are starting from an imminent terrorist threat and freezing, and possible confiscation, of crime related assets. The least pressuring priorities are related to threshold reports and gambling activity. The "case" analysis is then supplemented by information request through cooperation internationally and domestically as in case of TF and close liaison with the Security Intelligence Service. Final step of the FIU is to decide to open a criminal investigation for law enforcement agencies, disseminate information to ongoing cases, send information further for purpose of prevention and detection of illicit activity.

Based on the three options, the FIU is disseminating information of operational value to the local police departments, the NBI and the SIS which are responsible for operative support. While new criminal investigations and ongoing support are based on comprehensive analysis, the former step means that the FIU did not have necessary information or expertise for a final analysis and requested relevant authorities to take appropriate steps. In this way the Tax Office can order audits in suspicious companies, but these requests also include cases sent to the police for investigation. Therefore, in all the cases, law enforcement agencies receive relevant and polished information
for further actions. In addition, the FIU conducts strategic analyses on general trends and typologies, specific sectors, own performance and regional areas. These reports are then disseminated to the supervisory authorities, the Ministry of Foreign Affairs, the reporting entities and the public. In this way,

the FIU is supplementing the functionality of the AML/CTF model and follows the legally set requirements.

Judging from the current intelligence sharing procedures, the information flow within the Finnish AML/CTF model is structured in efficient way to gather information from the private and public sectors, remove unnecessary obstacle in analysis and reach relevant authorities. However, FATF analysis has outlined several issues in the cooperation between the officials what would be introduced in the next part.

FATF assessment of effectiveness in intelligence sharing

The FATF mutual evaluations are done by the group of experts coming from the other member states. The information is gathered through the questioners that are sent to national authorities, on-site interviews with AML/CTF representatives in various fields, national risk assessments and legal documents, relevant statistics and international reports on a country of interest. Consequently, gathered material is then evaluated across the FATF recommendations and international requirements for an exemplary AML/CTF system. However, reviewed documents and detailed analysis of problematic spots are not always specified in publicly available reports. Therefore, in exception of technical elements such as functions of the system and intelligence sharing, the outcomes of FATF report are difficult to verify as they include confidential information. Nevertheless, these outcomes and recommendations can provide guidance for a discussion on the identified problems. In general, Finnish AML/CTF have received mostly positive feedback from the evaluation committee. Some comments and suggestions for improvement were introduced for national policies, preventive measure, cooperation and supervision. At the same time many of the recommendations and gaps overlap with each other and improvement of one element can influence on several others.

Main points on intelligence sharing from the report relates to the cooperation side between the competent authorities and the FIU. As part of the assessment of the Finnish legal systems, the intelligence cooperation in financial intelligence and investigative activities have received a good mark and no significant gaps were identified by the assessors. Nevertheless, FATF report raises two important issues that are cooperation between the FIU with the supervisory authorities and the local police departments. Regarding the supervisors, FATF outlines that the dissemination of strategic reports from the FIU is taking place only between the FIU and the Financial Supervisory Authority, therefore, leaving aside the rest of the organisations. This finding is particularity problematic from the perspective of the functionality of the AML/CTF model, as without the comprehensive strategic updates, the supervising authorities are not fully able to upkeep the grasp of changing trends and developments in their respective fields of

supervision. In this way, the reporting entities are not being properly guided, what can influence on the amount and quality of the reports going back to the FIU. Nevertheless, FATF emphasize that situation is going to change with the new legislation, which will allow the FIU share the reports in more effective way.

In relation to the cooperation between the local police departments and the FIU, FATF has reached a conclusion that it is not sufficient enough and requires further improvement. The local police and the FIU are cooperating with each other on an ad-hoc basis as the information has to be requested from the FIU or it is disseminated in occasional way. Therefore, by looking at the number of ML investigations and how many of them relied on the FIU assistance, FATF points out that during the last three years (2015-2017) the share was not more than 40% (2016). In 2017 the percentage fell as low as 15% (only 34 out of 446) of cases that were relying on the FIU's information. In additional, the total figure of all the ML investigations and the FIU intelligence share is even less, coming to only 15% in 2015 and decreasing to 10% in 2017. This finding indicates that there is a gap in cooperation that can undermine the effectiveness of the AML/CTF and decrease the level of crime prevention in general. Criminal actors can more easily remain uncovered and investigations can take more time. Nevertheless, the only explanation provided by FATF is that possibly police officers are not well aware of the FIU functions. In this regard, this research aims to analyse the problem more detailly and provide potential explanation of underlying reasons for efficient cooperation.

Chapter 4: Analysis

Target-Oriented vs Outcome Oriented Approach

The FATF assessment methodology of effectiveness of an AML/CTF models uses national statistics as a main indicator of successful implementation of international AML/CTF standards and suitability of various elements in the system. By looking at the ML/TF convictions or opened investigations, it is possible to analyse the effectiveness of prosecution offices. In addition, Number of requests for cooperation and provided reports for ongoing investigations can help to evaluate the level of cooperation between various authorities. Also, court decisions on confiscation and freezing can outline how quickly can authorities react on ML/TF cases. Those are just few examples and other sources are comprehensively used in FATF analyses, but statistics remain in the central role. Moreover, the statistical analysis makes it possible to identify the gaps in the system and influencing reasons behind them. In case of Finnish financial intelligence cooperation and dissemination of information by the FIU, FATF reaches a conclusion that communication of the FIU with the supervising authorities and the local police departments requires further improvement. Concluding from the argument outlined above, the author of this research agrees that it is problematic that many supervising authorities are left without the strategic reports and decides to leave this question out of the scope of the analysis. However, the researcher believes that FATF conclusion that – "some police officers are not well aware of the work of the FIU and therefore are not using it to its full potential" (FATF 2019a, p. 60) – is not satisfactory and does not provide proper explanation. This conclusion seems to base on a prompt assumption with the only reference to the number of cases and the FIU officials, who underlined the moderate level of requests coming from the local police. Therefore, FATF concludes that "this fact might explain the modest overall share of ML investigations where financial intelligence was used" (Ibid)

This dissertation does not question the experience of the FIU officials and agree that the lack of knowledge of the work of the FIU might be an issue within the ranks of the police forces. Nevertheless, this work offers to approach the question from a slightly different perspective and analyse what other factors can potentially influence on efficiency and, therefore, effectiveness of cooperation. Contrary to the FATF outcome-oriented approach, it is aimed to analyse the issue from a broader perspective and incorporate the intelligence needs of the local police departments as a part of the larger crime and terrorism prevention. In this way, it is expected to answer the questions and understand: 1. why the police departments are not always using financial intelligence products of the FIU? 2. what factors influence on cooperation? 3. are cooperation and intelligence sharing actually inefficient? 4. what could be potentially improved? Therefore, this analysis will supplement the FATF report by setting its findings in alternative

lenses of inquiry. To begin with analysis of the intelligence needs it is decided to apply the framework of "target-centric approach" developed by Robert M. Clark (2013) to evaluate the relationship between the intelligence product consumers (local police) and intelligence collectors (FIU) within the linear structure of AML/CTF. The reason for this choice is that the traditional framework of intelligence cycle is oriented on policymakers (consumers) and hierarchical structures. However, crime and terrorism prevention include multiple consumers operating on the same objectives and therefore require structuring their intelligence collection and exchange in an auxiliary way.

Intelligence cycle in traditional framework starts from the needs of policy-makers that are then transferred to intelligence agencies planning and direction for collection activities. The objectives are distributed to intelligence collectors for information gathering. At the stage of processing intelligence agencies filter out all the relevant information and send it further for analysis. Finally, the polished intelligence product returns to the policymakers to support the decision-making process.
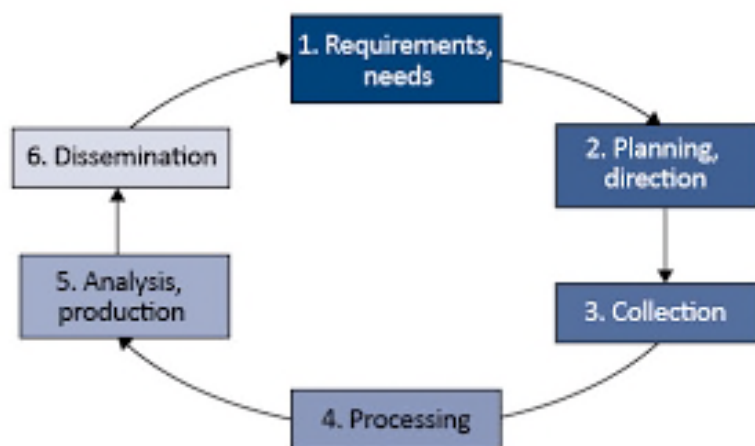
Figure 2: traditional intelligence cycle (Clark 2013, p.72)

As an alternative to traditional framework, Clark has offered a "Target Centred View" that aims "to construct a shared picture of the target, from which all participants can extract the elements they need to do their jobs and to which all can contribute from their resources or knowledge, so as to create a more accurate target picture" (2013, p. 81). Clark's original idea is that this form of thinking is more suitable for tactical and operational level, where rapid decisions have to be constantly made. Therefore, for example, geographically separated law enforcement agencies working on a same target (drug dealer) can contribute in coordinated investigation by providing physical surveillance on one side and communications intelligence on the other. Both of the LEAs can be interchangeably in roles of collectors and customers depending on the situation and the set objectives. In this way, the target-centric approach brings together all the relevant stakeholders, which have a shared knowledge of a target. This also provides opportunities to guide intelligence gathering and dissemination in more precise way, starting

from the gaps in knowledge of a consumer that are then filled by the collectors and vice versa. Shared knowledge promotes the ability of analysts to proactively identify the needs of information and obtain it from relevant sources as well as obtain the details from customers themselves.
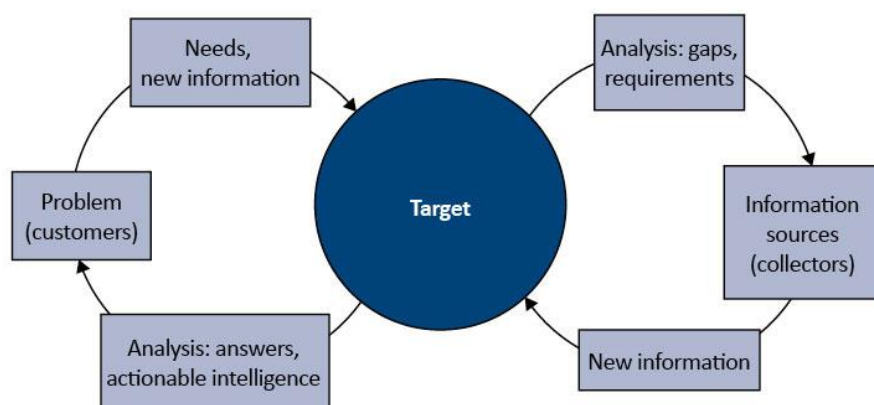

Figure 3: a target-centred intelligence cycle (Clark 2013, p. 83)

Coming back to the AML/CTF models and financial intelligence sharing, it can be therefore be concluded that – by setting the investigative authorities in a place of consumers and the FIU in a role of an analyst working together on the same objectives of ML/TF and terrorism/crime prevention – it is possible to broadly assess the flow of information between the organisations. With the large access to databases (including the police) and the reporting entities as collectors, the FIU's function is purely analytical and supportive for criminal investigations. It also has to notify the security agencies in case of a new criminal case, relevant information, or unclear and suspicious leads. In addition, a target for consumers, analysts and collectors is an individual or any organisation which tries to disguise origin of illicit money and/or move, raise and provide funds for terrorist purposes. By taking this approach in next chapter, it will be tried to analyse why financial intelligence is not always used by the local police departments.

Why Not to Use Financial Intelligence?

Within the Finnish national security structure and AML/CTF more specifically there are three central players with investigative powers – the Security Intelligence Service, the National Bureau of Investigations and the local police departments. This is not to say that Customs or the Border Guard are

less relevant but to emphasise the responsibility and powers to bring criminals and terrorists to justice. Although the Border Guard and Customs have some investigative powers on money laundering cases, eventually all the criminal investigations are done by the police for further prosecution and arrests, if necessary. Therefore, in case of crime and terrorism prevention, also other government organisations fall into the role of supportive collectors and analysts. the SIS, the NBI and the police departments are therefore the main intelligence consumers. At the same time, also the consumers have to grant access to information in their possession to each other and analysts to various extent.

In the context of intelligence needs, a broad concept of "crime and terrorism prevention" is not helpful and requires further breakdown to see who is doing what and what is needed. The National Counter Terrorism Strategy (Sisäministeriö 2018) set four strategic objectives, which are "prevention", "incident management", "combating" and "detection" of terrorist activities. While prevention and incident management concentrate on "de-radicalisation" and societal preparedness for serious incidents, detection and combating directly relate to the work of the security agencies. Form the three investigative authorities, terrorism detection and combating fall into the scope of responsibilities of the Security Intelligence Service and National Bureau of Investigation. The SIS is responsible for counter intelligence and terrorism, regional surveillance and security clearance. But with new legislation in 2019 (SUPO 2019), the SIS powers also include "digital services" (comint), foreign intelligence and information gathering. The SIS is then responsible for monitoring the terrorist suspects and intelligence sharing home and abroad. On the other hand, the NBI's main tasks are to "combat international, organised, professional, financial and other serious crime" (Suomen Poliisi 2019) nationwide. The NBI is also conducting investigations on terrorist suspects and maintain close relationship with the SIS through liaison persons (FATF 2019a, p. 56).

Finland has 11 police departments with main tasks of "license services", "maintaining public safety and security", "crime prevention" and "traffic security" (Suomen Poliisi 2019). More precisely, the local police share its part in organised crime prevention and adopts a "follow the money" approach. The "Police Strategy" document (Suomen Poliisi 2017) outlines among others two important objectives of police activities in form of "promotion of security" and "crime prevention". The promotion of security includes tasks to prioritising and upkeeping central functions in crime prevention, utilisation of digital sources in intelligence-led approach, and establish cooperation in accordance to the needs and security environment in the area of monitoring. In crime prevention, the emphasis is on the improvement of criminal investigation processes, serious crime prevention with a focus on international developments, and improvement of cyber-crime prevention techniques. The police departments cooperate with each other, the NBI and maintain relationship to their counterparts internationally. The Security Intelligence

Service emphasises that it works in close cooperation with the local police as for example on surveillance of potential suspects with terrorist connections (SUPO 2018). However, the author estimates that the local police departments are in a supplementary role and have no access or need for the TF intelligence information coming from the FIU.

Judging from the general objectives and specific responsibilities of the security agencies, it is possible to identify that they cover a wide range of illicit activity and their tasks partially overlap between the organisations. Therefore, in order to meet the strategic objectives and cover operational needs, the security professional require wide source of information. From an ML/TF perspective, required financial information relates to terrorist activity (SIS and NBI) and serious corruption, market abuse and financial crimes, and money laundering (the NBI). At the same time, money laundering and financial crimes are also in the scope of the local police departments as part of the "grey economy" and organised crime prevention. Moreover, from the "reactive" and "proactive" approaches this information should serve to identify and investigate the crimes that already happened (reactive) and prevention of new ones from happening (proactive). Therefore, the FIU is in a central position to provide quality intelligence product coming from the financial sector.

During this analysis it was possible to identify three problematic spots that potentially influence on the level of cooperation between the local police and the FIU. Those are – access to data, other intelligence channels and differing objectives between the security agencies. All of the mentioned gaps are interrelated and improvement of one might fix the other. The access to data is the first identified issue, which might have negative impact on direct police/FIU cooperation. The FIU has a wide access to databases and receives a wide variety of reports coming from the private and public sources. In this way, the FIU has an ability to obtain a comprehensive understanding of a target individual, network, or organisation and their illicit activities. By cross-checking the received information, the FIU is able to evaluate whether this information relates to an ongoing investigation or a new crime and terrorist activity. After careful analysis, the information is then disseminated to the relevant authorities. Nevertheless, part of the arriving information and "money-laundering" register is only available to the FIU and is out of the reach of the police forces. As identified by FATF, "STRs" and "threshold reports" are not available to the police and information is granted only by request.

This setting is particularly problematic from the "target-centric" approach. Limited access to information sets the LEAs and the FIU on different levels of knowledge, what also means that the analysts and consumers have different view and understanding of the target(s). While analysts may identify the dots between a transaction and predicate crime/terrorist activity and send this information further, the FATF

report outlines that the support of ongoing investigations of the local police is occasional in nature. Therefore, information will not be consumed until requested. At the same time, the requirement to request information is problematic due to the limited knowledge what information is available, if anything. Lack of a comprehensive picture of a target and therefore understanding of the needs may increase the threshold for cooperation. Moreover, the FIU and the NBI can request additional information from all the reporting entities but there is no clear description what powers are in possession of the local police. Conclusively, because of the delays in dissemination, the intelligence product might lose its relevancy and usability.

On the other hand, in the wide structure of national security and AML/CTF network, the intelligence consumers are not limited only to one analyst and can even avoid this step by interacting directly with the collectors. The SIS, the NBI and the police departments have their own units of analysis and instruments for intelligence collection. In addition, access to financial information varies to an extent between the three and includes similar databases and collectors in possession of the FIU. For example, from the listed registers (see previous chapter) available to the FIU, at least 80% are also in use within the police forces. This observation is supported by the objectives set in the national guiding documents, tasks related to the security services, forms of cooperation (will be discussed below), and other information in personal possession. Moreover, according to the FATF report, compliance reports and cross-border cash movement declarations are directly available to the law enforcement agencies. Judging from the available access of data and collectors, the LEAs and more specifically the police departments are able to an extent independently fill the gaps in their knowledge about the target(s). In addition, mutually available collectors can contribute directly to the investigations and intelligence efforts. Therefore, the main intelligence consumers are not always dependent on the FIU, what again can decrease the level of cooperation as there are less gaps to fill in financial dimension.

The access to data and relevant information also relates to various forms of intelligence channels between the intelligence consumers themselves. In the flat "target-centric" intelligence cycle, consumers can also become analysts and collectors or combine multiple roles at the same time. In a complex national security environment, various cooperation arrangements are becoming more relevant and take place in bi-lateral and multilateral partnerships beyond and across national and international organisations. Finnish authorities extensively cooperate through international organisations of Interpol and Europol, as well as have established connections with the Nordic countries and Russia, for example. Most importantly there is a sing of healthy cooperation between the national security services as for instance in the so-called "PTR-cooperation" (Suomen Poliisi 2019, p. 26). Coming from the letters of three founding organisations in 2004 – Police, Customs (Tulli) and Border Guard (Rajavartiolaitos) – PTR partnership aims to

maintain a real time situational awareness through the PTR centre for criminal intelligence and "sea, land and air traffic" special units. Later in the process, the NBI has joined the partnership and it is now leading the PTR centre for criminal intelligence. Conclusively, cooperation activities promote the emergence of new channels for flow of intelligence and additional contribution to the target orientation. Therefore, the intelligence consumers can directly share their knowledge and outflank unnecessary interaction with analysts (e.g. the FIU). This can also help to avoid restrictions of access to data as in case of formalities in requests to the FIU. Being part of the NBI and having few of its officer on part-time seconded positions within the Bureau (FATF 2019, p. 60), the FIU's information is easily available to other units. At the same time this information can be shared further to the local police through the PTR or on a bi-later basis.

Finally, the security agencies have different tasks and objectives set to their fields of responsibilities. While financial crimes and "grey economy" certainly remain at the centre of objective for law enforcement, money laundering related to other predicate crimes might receive less attention. This is for the reason that the Finnish AML/CTF does not prosecute self-launderers and TF charges are not applicable to the convicted terrorists. Therefore, predicate crimes themselves plays more important role in crime prevention. Although assisting ML individual or terrorist sympathisers are in the scope of criminal investigations and prosecution, they cannot be sentenced before a predicate crime or terrorist activity are clearly identified. Moreover, the security agencies conduct investigations on other crimes and apply multiple techniques for intelligence collection. Obtained pieces of information from communication intelligence, human sources, home searches and digital devices can equally provide information on illicit money and financial assets. In this way, the intelligence consumers are themselves able to identify the needs of intelligence product on a target(s) and satisfy them through their own collection activities. In addition, from a strategic point of view, the FIU conducts various strategic reports and disseminate them to relevant organisations. The FATF report mentions only the supervising authorities but emphasises that, due to the changing secrecy law, the FIU will be able to share them more widely. Although it is not clear if the police departments get access to the reports, it is possible to assume that the NBI is included in dissemination and at least indirectly contributes to the shared knowledge of operational environment.

Nevertheless, few issues may arise from insufficient use of the FIU knowledge. First, collection of an information by the local police may take more time, while it is already available in form of a final intelligence product on request. Therefore, available resources could be put in more important use and decrease time of criminal investigations, which already have enormous length as in case of financial crimes (Koivisto 2017, p. 23). Second, intelligence information arrives through many channels in different form and shape, and its analysis might lead to various outcomes than in the FIU reports. A possible lack of expertise within the local police and different access to data pose a risk of misinterpreting

information or leaving aside an important lead. In addition to the problems with time and resources, this issue is even more important as it means that some crimes or illicit activity may stay uncovered. Third, in terms of reactive and proactive crime prevention, a lack of efficient communication between the FIU and the local police (and LEAs in general) could mean that the investigative authority will lose part of their capability in both dimensions. Terrorist or criminal cells can remain active after being uncovered and try various ways to move their money around. In this way disconnecting the whole structure of collectors (reporting entities) and analyst (the FIU) will remove important red flags and indicators for the investigators.

In conclusion, as a result of the analysis, the target-oriented approach demonstrates well that national statistics do not necessary reveal the underlying reasons behind the "effectiveness" of cooperation between the organisations in AML/CTF but also in a broader security network. Although numbers can outline the problematics spots and shifts in the AML/CTF structure – as in case with decrease/increase in reporting figures or lack of reports in some particular fields – it is necessary to put these findings in a broader perspective. Therefore, a moderate number of requests from the local police to the FIU can hide in other sources of intelligence, forms of cooperation, and intelligence needs. Moreover, there is no clear limit as to what should be considered as a sufficient amount of requests. If an aim is to use the knowledge of the FIU in all the criminal investigations, then what should be done if a piece of necessary information is already obtained? Or there is no need to gather additional data? In this way, this procedure will unnecessarily spend the resources of the FIU with only slightly more than 20 officers and a large amount of incoming material. Nevertheless, the operational level and issues lead to another important question: what other structures can influence on intelligence sharing?

Financial Intelligence Sharing and Structural Factors

In the previous discussion, it was aimed to identify the main channels of intelligence information and operational issues, which might potentially influence on efficiency and effectiveness of flow of financial intelligence between the local police and the FIU. Nevertheless, flow of information and existing channels do not outline the whole picture of intelligence cooperation as national security structures can have various obstacles, which prevent and influence on effective intelligence sharing. The evaluation theories of network analysis and inter-organisational cooperation have developed a range of perspectives on internal and external factors, by looking at outcomes, processes and structure (Provan and Sydow 2009). As a result, various issues of competition, secrecy, trust, interests and power were outlined in different forms of partnership and models. Iztok Prezelj (2014, p. 327) writes that among others

"cooperation evolves according to the perceived threats, needs, opportunities, and inter-organisational chemistry". This statement indicates that there are no single methods of analysis and different networks include different factors, and therefore will lead to diverse conclusions. Results of an analysis depend on whether a researcher looks at organisations, individuals, or structure, and apply "bottom to up" or "up to bottom" perspective (Provan and Sydow 2009). However, while people shape organisations, it is organisations which guide individual's behaviour and structure which determines the types of partnership. Therefore, it might be even more important to look at the external factors.

Regarding the cooperation matters between the FIU and the police departments, this part of the work aims to address how structural settings in national security and AML/CTF influence on cooperation, and what consequences does it have for previously discussed flows of information. In this way, the goal is to identify potential obstacles in the system in order to discuss efficiency questions in the following part. By structure it is meant the specific arrangements between the security organisations to meet the objectives and requirements. These arrangements include location of the FIU, shared responsibilities, and management or coordination of the cooperation efforts. In the assumption of this research, these three external factors play a key role in formation of working AML/CTF models as they determine the level of tensions, clashes of interests and achievement of mutual goals. The objectives are still the same. and they are crime prevention and investigation as well as identification of money laundering. Terrorist financing is excluded for the reason that in counter-terrorism investigations the FIU cooperates mostly with the SIS and the NBI.

Starting from the location of the FIU, it is within reach to notice that there are certain strengths and limitations. As a part of the NBI, the FIU is a law enforcement type of financial intelligence gatherers and therefore can effectively supplement the work of the LEAs. It has access to the criminal intelligence and can disseminate suitable reports for criminal investigations. Consequently, the FIU is a part of a network of security agencies what also increase a level of trust, precision of information and dialogue between the agencies, and promote mutual understanding of shared objectives. However, although the FIU is established as an independent body, its physical presence at the premises of the NBI might create obstacles to various extent. In simple terms, while being a part of law enforcement network, the FIU is separated from the local police departments and their interaction is limited and take place on an ad-hoc basis. The officers from the FIU rotate between the positions within the NBI and also have direct access to the liaison person from the SIS. At the same time, physical distance from the police departments decrease the level of personal connection and upkeep the formal format for intelligence sharing. Therefore, formal requests and occasional dissemination of information to the local police prevent the organisations from developing a lasting relationship and incorporate processes of intelligence sharing in a

more unfired way. This setting forms a problem mostly on a side of the local police and arguably might leave it without financial intelligence information. The FIU still has access to information for its analyses.

On the other hand, the location of the FIU raises the issues of secrecy, trust and competition coming from the shared responsibilities. Even as an individual body, the FIU is still required by law to provide assessments of its performance to the board of the NBI (Act 445/2017). Therefore, the FIU is partially under control of the Bureau, which can then use it in accordance to own interests. This is for the reason that the local police departments and the NBI have overlapping functions in prevention of organised and financial crimes as well as money laundering. In this way, there is a danger of growing competition and limited intelligence sharing between the organisation, which can try to promote and keep information mostly to their own units. In this way, the FIU will be perceived as an integral part of the competing agency, what also partially fits with the FATF conclusion that the police officers "are not well aware of the FIU's functions". The growing competition can then influence on the level of trust between the FIU and the local police, and influence on wider secrecy measures on one side or another. Judging from statistic, it is hard to measure the level of trust, but still relevant scandals related to the senior officer from the drug enforcement unit of the Helsinki Police Department (Happonen 2019) will unavoidably have an impact on forms of cooperation of the local police with the NBI. During the mutual investigation on the international drug trade network, the leading officer from the HPD was himself involved in the criminal network and mislead the investigation by various means.

The issues of trust, competition and secrecy can be solved with the proper supervision of the cooperating authorities. In the Finnish AML/CTF model, a general coordination of mutual efforts between the AML/CTF related organization is done by the Ministry of Interior. On the Ministry's website (Sisäministeriö 2019) it is stated that this coordination "involves all the competent authorities as it is defined in the act on Preventing of Money Laundering and Terrorist Financing". However, the act (444/2017) itself does not provide a proper definition of the competent authorities and it remains unclear, which organisations are actually included in the supervisory framework. While there is a good level of supervisory coverage by the authorities over the reporting entities, this research estimates that there is no permanent coordinating body for direct cooperation between the FIU and the local police. On the other hand, the Finnish Police Forces are under the control of the National Police Board, which is responsible for guidance, planning, development and supervision of the LEAs (Suomen Poliisi 2019). It also decides on cooperation between the LEAs including the National Bureau of Investigations, what can more actively promote the involvement of the FIU in the police work. However, as the FIU is an independent organisation, the guidance of the unit through the broader framework of law enforcement cooperation leads back to the problem of competition between the LEAs and shifting the FIU towards tighter control

of the NBI. In this way, without the proper guidance, the local police and the FIU have to build their relationship independently. This in turn can lead to even more inefficient level of communication.

Finally, – in light of a wider national security structure, information channels, intelligence needs and potential structural obstacles – it is possible to conclude that the FIU/local police intelligence sharing is not build on a lasting foundation, and interaction take place only in case of colliding objectives of the local police or legally required dissemination of intelligence by the FIU. Therefore, the type of partnership is ad-hoc in nature and it is a potential gap in the Finnish AML/CTF model. Structural factors create an additional negative influence on already discussed access to data, intelligence channels and flow of information more broadly. The main problem is that, combined together, the whole discussion lead to a conclusion that there is possibility of interruptions in intelligence sharing between the local police and the FIU, and this conclusion is consistent with the FATF report. However, contrary to FATF, the analysis in this work outlined more broader set of issues than the lack of sufficient knowledge of the FIU within the ranks of the police.

Is Intelligence Sharing Actually Inefficient?

At the beginning of the research project, a range of objectives were set to answer the question: how efficient is the flow of information and cooperation between the local police departments and the financial intelligence unit? In this way, the research question includes two interrelated but still separate parts of "information flows" and "cooperation". In addition, these parts are approached from the lenses of efficiency instead of effectiveness. According to the Oxford Learner's Dictionary (2019), efficiency means "the quality of doing something well with no waste of time or money". In this way, efficiency relates to aims of an organisation to achieve more objectives with less input of resources. On the other hand, effectiveness means "the fact of producing the result that is wanted or intended" (Ibid) and, therefore, it is clearly output oriented. As with intelligence channels and cooperation, effectiveness and efficiency are closely interconnected. Therefore, the aim of the work were to supplement the FATF report and go deeper into the process and structure.

In regard to flow of information, the definition of efficiency underlines the needs of uninterrupted flow of intelligence between the FIU and the local police for successful criminal investigations of ML/TF and other crimes more broadly. Based on the previous analysis, it is estimated that in a broader national security structure, the flow of intelligence is efficient and is able to satisfy the requirements of the police and close the gaps in knowledge. A wide access to databases, other sources of information, and cooperation with partially the same intelligence collecting and analysing organisations, which are

available to the FIU, the local police is able to fulfil its tasks. Therefore, there is no significant threat to crime prevention capabilities and pressure to request the information from the FIU. However, the FIU is still a valuable source of intelligence with relevant expertise and a wide reach over the reporting entities. From this perspective, – due to potential negative impact on the length of investigations and decrease of proactive/reactive capabilities – the maintenance of FIU/local police communication is still necessary. Here, this dissertation concludes that the direct intelligence sharing between the FIU and the police departments is less efficient or might even reach a level of "inefficient", depending on the perspective.

The FATF identified that over the period of three years (2015-2017) the LEAs have utilised only 10-20% (2015:15%, 2016:20%, 2017:10%) available of the available FIU intelligence in the total amount of ML/TF investigations. The report provides a table with statistics of ML investigations braked by the aggravated, no aggravated and other money laundering offences. However, it is not clearly stated how many of the cases were led by the local police and how many by the NBI. But in light of the percentage, figures still emphasise the low amount of requests. Taking into account that the FIU is in close day-to-day cooperation with the NBI, these statistics might be even lower for the local police. Altogether, including the statistical outcomes, structural obstacles, and processes this work reaches a paradoxical challenge of what influence on what. Numbers indicate low cooperation, operational arrangements demonstrate good level of available information, but structure can again limit intelligence sharing and cooperation. Therefore, there is no clear answer of effectiveness and efficiency in a wider network. However, by concentrating on the main research question, the local police departments and the FIU, this dissertation concludes that cooperation between the two is not satisfactory.

The access to databases, other intelligence channels and cooperation, or even more importantly structural factors do not improve the efficiency of intelligence sharing of the organisations under study. Judging from this, out of all the possible options, the final conclusion is that the main issue for effective/efficient intelligence sharing and cooperation is the current formal or restricted way of exchanging information. Coming back to the "target-centric" approach, the requirement to fill the request to the FIU or occasional dissemination of information prevent the organisations from developing a real-time shared knowledge of a target (criminals). This poses a problem on the both sides. Although the FIU is legally required to analyse and send intelligence products to the security agencies, this mostly happens in case if a new lead emerges while there is an ongoing investigation, or a suspicious case is being escalated and sent further. But what happens if a criminal investigation is initiated by the local police around the financial intelligence unit? As a result, a raw intelligence information in possession of the FIU will not be analysed and consequently disseminated. On the other hand, the local police is not aware of the available intelligence data and will not be able to independently identify the gaps for further request.

Recommendations

The final conclusion that the FIU and the local police departments is undermined by the insufficient current process of intelligence sharing is also to an extent consistent with the FATF report. The potential lack of knowledge of the work of the FIU can be reasonably explained by low amounts of intelligence requests. This is for the reason that the FIU is required to provide intelligence reports but is not able to do that proactively for all the investigations. Therefore, one of the possible recommendations is to promote knowledge and encourage the police to fill the requests more actively. In this way, shared knowledge will be constantly updated, and the gaps will be filled on a timely basis. This should be done by the more active engagement of the FIU with the local departments. At the same time, the automatization of the request procedures poses a risk of unnecessary requests and unnecessary spending of the resources of the FIU. But this again can be solved by the natural and documented formulation of guidelines. Another option would be expanding the access of the police to the FIU information or notification procedures of newly initiated ML/TF investigations. The FIU has a direct access to the police systems and filter out the incoming information. In this way, information would effectively circulate between the FIU and the local police as well as again promote knowledge of the LEA officers.

Theoretical Considerations and Further Research

This research approached the question of efficient intelligence sharing and cooperation within the Finnish AML/CTF model. In order to analyse, understand and identify the potential problems, it was decided to apply a framework of "target-centric" intelligence and go through the operational issues between the local police departments and the financial intelligence unit. Therefore, the perspective was on the availability, flows, restrictions and channels of financial intelligence in a wider security network. The security organisations were interchangeably set in roles of intelligence consumers, collectors and analysts to identify the needs and requirements of the ones under study. Further, based on the discussion, structural obstacles for intelligence sharing were also considered. However, this research does not aim to provide a comprehensive explanation of all the potential factors, therefore, leaving aside individual and organisational aspects. Due to the bureaucratic challenges, the author of this work was not able to conduct interviews with the Finnish security professionals and expand this research more detailly on influential internal factors within and between the organisations. Therefore, further research is required on the National Bureau of Investigation, police departments individually, and national security network more widely. In this way, it would be possible to supplement the identified findings and put them into alternative perspective.

Conclusion

Over the last 30 years, the international AML/CTF standards have witnessed a rapid improvement to counter money laundering and terrorist financing, as well as related illicit behaviour. The scope of international and national AML/CTF regimes include a wide range of predicate crimes and sophisticated techniques for the crime and terrorism prevention. The international organisations, regional bodies and national states are constantly adapting their tactics and strategies to promptly changing criminal activity, and aim to improve all the aspects of this challenging work. Although, a lot of improvements have been achieved, the question of enormously large flows of illicit funds is far from being resolved. Terrorist and criminal actors adopt their methods in order to remain discrete and avoid attention of the law enforcement and intelligence agencies. In this way, criminal activity aims to take advantage of possible gaps in the AML/CTF structures and financial sectors more widely. Therefore, it is significantly important to integrate the AML/CTF procedures into the wide national security structures. At the same time, constant assessment of the AML/CTF is required to identify its weak points and take appropriate actions. This notion is especially relevant to intelligence sharing and cooperation between the financial intelligence units and law enforcement agencies. Criminal investigations require a wide range of intelligence information and, as it was demonstrated in this research, potential interruptions in information exchange might lead to negative consequences. Therefore, constant connections and effective cooperation between the law enforcement agencies and the financial intelligence units is required to be maintained further.

BIBLIOGRAPHY

Act 39/1889. *Suomen Rikoslaki [Criminal Code of Finalnd]*. [online] Available at: <https://www.finlex.fi/fi/laki/kaannokset/1889/en18890039> [Accessed 18 June].

Act 444/2017. *Laki Rahanpesun ja Terrorismin Rahoittamisen Estämisestä [act on Preventing of Money Laundering and Terrorist Financing]*. [online] Available at: <https://www.finlex.fi/fi/laki/alkup/2017/20170444> [Accessed 18 June 2019].

Act 445/2017. *Laki Rahanpesun Selvittelykeskuksesta [Act on the Financial Intelligence Unit]*. [online] Available at: <https://www.finlex.fi/fi/laki/alkup/2017/20170445> [Accessed 18 June 2019].

Alpert, P. G., and Dames, M., 2011. Intra-Agency and Inter-Agency Cooperation in International Police Work. *Police Practice and Research: an International Journal* 12(2), pp.104-106.

Armey, L., and Melese, F., 2018. Minimizing Public Sector Corruption: The Economics of Crime, Identity Economics, and Money Laundering. *Defence and peace Economics* 29(7), pp.840-852.

Arpajaishallinto, 2019. *Terrorismin Rahoitus ja Yleishyödylliset Yhteisöt [Terrorist Financing and NGOs]*. Arpajaishallinto. [online] Available at: <https://www.arpajaishallinto.fi/instancedata/prime_product_julkaisu/intermin/embeds/arpajaishallintow wwstructure/14765_Terrorismin_rahoitus_ja_yleishyodylliset_yhteisot.pdf?bdadc3b8c5b0d588> [Accessed 26 June 2016]. (in Finnish).

Arquilla, J., 2002. It Takes a Network. *RAND*. [online] Available at: < https://www.rand.org/blog/2002/08/it-takes-a-network.html> [Accessed 19 June 2019].

Bagella, M., Busato, F. and Argentiero, A., 2013. Using Dynamic Macroeconomics for Estimating Money Laundering: A Simulation for the EU, Italy, and the United States. In: B. Unger, & D. van de Linde, ed. 2013. *Research Handbook on Money Laundering*. UK/USA: Edward Elgar Publishing Limited.

Bartlett, B.L., 2002. The Negative Effects of Money Laundering on Economic Development. *Platypus Magazine* 77, pp.18-23.

BBC, 2018. Panama Papers: Four Charged in US With Fraud and Tax Evasion. *BBC.* [online] Available at: < https://www.bbc.com/news/world-us-canada-46449696> [Accessed 20 July 2019].

Bernstein, J., 2017. *Secrecy World: Inside the Panama Papers Investigation of Illicit Money Networks and the Global Elite.* New York: Henry Holt and Co.

Brzoska, M., 2016. Consequences of Assessments of Effectiveness for Counterterrorist Financing Policy. *Administration and Society* 48(8), pp.911-930.

Campbell, D., 2019. Inside the 21st-century British Criminal Underwolrd. *The Guardian.* [online] Available at: <https://www.theguardian.com/world/2019/jul/04/inside-the-21st-century-british-criminal-underworld> [Accessed 5 July 2019].

Carter, L. D., 2009. *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies.* 2nd ed. Michigan: U.S. Department of Justice.

Cassara, J., and Jorisch, A., 2010. *On the Trail of Terror Finance: What Law Enforcement and intelligence Officers Need to Know.* Washington, DC: Red Cell Intelligence Group.

Clark, M. R., 2013. *Intelligence Analysis: A Target-Centric Approach.* 4th ed. US: SAGE Publications Inc.

Council of Europe, 2019. MONEYVAL in Brief. *Council of Europe.* [online] Available at: < https://www.coe.int/en/web/moneyval/moneyval-brief> [Accessed 27 June 2019].

Croissant, A., and Barlow, D., 2007. Following the Money Trail: Terrorist Financing and Government Responses in Southeast Asia. *Studies in Conflict and Terrorism* 30(2), pp.131-156.

Deleanu, I., 2013. The Role of Information for Successful AML Policy. In: B. Unger, & D. van de Linde, ed. 2013. *Research Handbook on Money Laundering*. UK/USA: Edward Elgar Publishing Limited.

D'Souza, M. S., 2008. Indo-US Counter-Terrorism Cooperation: Rhetoric Versus Substance. *Strategic Analysis* 32(6), pp.1067-1084.

Egmont Group, 2019a. Financial Intelligence Units (FIUs). *Egmont Group.* [online] Available at: < https://egmontgroup.org/en/content/financial-intelligence-units-fius> [Accessed 5 June 2019].

Egmont Group, 2019b. About the Egmont Group. *Egmont Group.* [online] Available at: < https://egmontgroup.org/en/content/about> [Accessed 5 June 2019].

Egmont Group, 2019c. Document Library. *Egmont Group.* [online] Available at: < https://egmontgroup.org/en/document-library> [Accessed 5 June 2019].

European Commission, 2019. Financing of Terrorism. *EC.* [online] Available at: < https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/financing_en> [Accessed 18 June 2019].

European Union, 1991. *Council Directive on Prevention of the Use of the Financial System for the Purpose of Money Laundering (91/308/EEC).* Official Journal of the European Communities. [online] Available at: < https://eur-lex.europa.eu/resource.html?uri=cellar:57ce32a4-2d5b-48f6-adb0-c1c4c7f7a192.0004.02/DOC_1&format=PDF> [Accessed 20 June 2019].

European Union, 2001. *Directive 2001/97/EC of the European Parliament and of the Council Amending Council Directive 91/308/EEC on Prevention of the Use of the Financial System for the Purpose of Money Laundering.* Official Journal of the European Communities. [online] Available at: < https://eur-lex.europa.eu/resource.html?uri=cellar:57ce32a4-2d5b-48f6-adb0-c1c4c7f7a192.0004.02/DOC_1&format=PDF> [Accessed 20 June 2019].

European Union, 2005. *Directive 2005/60/EC of the European Parliament and of the Council on the Prevention of the Use of the Financial System for the Purpose of Money Laundering and Terrorist Financing.* Official Journal of the European Communities. [online] Available at: < https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005L0060&from=EN> [Accessed 20 June 2019].

European Union, 2001. *Council Framework Decision on Money Laundering, the Identification, Tracing, Freezing, Seizing and Confiscation of Instrumentalities and the Proceeds of Crime (2001/500/JHA).* Official Journal of the European Communities. [online] Available at: < https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001F0500&from=GA> [Accessed 20 June 2019].

European Union, 2015. *Directive (EU) 2015/849 of the European Parliament and of the Council on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing, Amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.* Official Journal of the European Communities. [online] Available at: < https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L0849&from=EN> [Accessed 20 June 2019].

European Union, 2018. *Directive (EU) 2018/843 of the European Parliament and of the Council Amending Directive (EU) 2015/849 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing, and Amending Directives 2009/138/EC and 2013/36/EU.* Official Journal of the European Communities. [online] Available at: < https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L0843&from=EN> [Accessed 21 June 2019].

EUROPOL, 2019. *EU Terrorism Situation and Trend Report.* Hague: EUROPOL [online] Available at: < https://www.europol.europa.eu/activities-services/main-reports/eu-terrorism-situation-and-trend-report> [Accessed 30 March 2019].

EUROPOL, 2015. *Why is Cash Still King? a Strategic Report on the Use of Cash by Criminal Groups as a Facilitator for Money Laundering.* EUROPOL. [online] Available at: <https://www.europol.europa.eu/publications-documents/why-cash-still-king-strategic-report-use-of-cash-criminal-groups-facilitator-for-money-laundering> [Accessed 6 June 2019].

FATF, 2019a. *Anti-Money Laundering and Counter Terrorist Financing Measures – Finland. Fourth Round Mutual Evaluation Report.* Paris: FATF. [online] Available at: < http://www.fatf-gafi.org/countries/#Finland> [Accessed 7 July 2019].

FATF, 2019b. *What is Money Laundering?.* FATF. [online] Available at: <https://www.fatf-gafi.org/faq/moneylaundering/> [Accessed 10 July 2019].

FATF, 2019c. *Terrorist Financing Risk Assessment Guidance.* Paris: FATF. [online] Available at: < http://www.fatf-gafi.org/publications/methodsandtrends/documents/terrorist-financing-risk-assessment-guidance.html> [Accessed 11 April 2019].

FATF, 2019d. *International Standards on Combating money Laundering and the Financing of Terrorism and Proliferation.* Paris: FATF. [online] Available at: < http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html> [Accessed 28 May 2019].

FATF, 2019e. Who We Are. *FATF.* [online] Available at: <http://www.fatf-gafi.org/about/> [Accessed 10 June 2019].

FATF, 2019f. Members and Observers. *FATF.* [online] Available at: <http://www.fatf-gafi.org/about/membersandobservers/> [Accessed 10 June 2019].

FATF, 2019g. High-Risk and Other Monitored Jurisdictions. *FATF.* [online] Available at: < http://www.fatf-gafi.org/countries/#high-risk> [Accessed 15 June 2019].

FATF, 2008. *Proliferation Financing Report.* Paris: FATF. [online] Available at: < http://www.fatf-gafi.org/publications/methodsandtrends/documents/typologiesreportonproliferationfinancing.html> [Accessed 20 April 2019].

FATF, 2018. *Professional Money Laundering.* Paris: FATF. [online] Available at: < http://www.fatf-gafi.org/publications/methodsandtrends/documents/professional-money-laundering.html> [Accessed 20 April 2019].

FATF, 2007. *Annual Review of Non-Cooperative Countries and Territories 2006-2007: Eighth NCCT Review.* Paris: FATF. [online] Available at: < http://www.fatf-gafi.org/media/fatf/documents/reports/2006%202007%20NCCT%20ENG.pdf> [Accessed 15 June 2019].

Ferwerda, J., 2013. The Effects of Money Laundering. In: B. Unger, & D. van de Linde, ed. 2013. *Research Handbook on Money Laundering.* UK/USA: Edward Elgar Publishing Limited.

Ferwerda, J., 2009. The Economics of Crime and Money Laundering: Does Anti-Money Laundering Policy Reduce Crime?. *Review of Law and Economics* 5(2), pp.903-929.

Garside, J., 2019. Q&A: What is the "Troika Laundromat" and How Did It Work?. *The Guardian.* [online] Available at: < https://www.theguardian.com/world/2019/mar/04/qa-what-is-the-troika-laundromat-and-how-did-it-work> [Accessed 5 July 2019].

Goodman, M., 2015. *Future Crimes*. US: Doubleday.

Groot, L., 2013. Money Laundering, Drugs and Prostitution as Victimless Crimes. In: B. Unger, & D. van de Linde, ed. 2013. *Research Handbook on Money Laundering*. UK/USA: Edward Elgar Publishing Limited.

Habib, B., 2015. The enforcement problem in Resolution 2094 and the United Nations Security Council sanctions regime: sanctioning North Korea. *Australian Journal of International Affairs* 70(1), pp.50-68.

Happonen, P., 2019. *Aarnio istuu 13 vuoden vuomiosta nyt 3 vuotta, miten se on mahdollista?* [*Aarnio Will Werve Only 3 Years out of His 13 Year Sentence. How is That Possible?*]. *Helsingin Sanomat*. [online] Available at: < https://yle.fi/uutiset/3-10851137> [Accessed 20 July 2019]. (in Finnish).

Harding, L., 2017. The Global Laundromat: How Did It Work and Who Benefited?. *The Guardian*. [online] Available at: < https://www.theguardian.com/world/2017/mar/20/the-global-laundromat-how-did-it-work-and-who-benefited> [Accessed 20 June 2019].

Harvey, J., 2004. Compliance and Reporting Issues Arising for Financial Institutions from Money Laundering Regulations: A Preliminary Cost Benefit Study. *Journal of Money Laundering Control* 7(4), pp 333–346

Huhtamäki, H., 2019. Käsikranaateista Tuli Arkea Ruotsissa [Hand Granades are a New Normal in Sweden]. *Helsingin Sanomat*. [online] Available at: <https://www.hs.fi/ulkomaat/art-2000006180564.html> [Accessed 20 June 2019]. (in Finnish)

Hunt, J., 2011. The New Frontier of Money Laundering: How Terrorist Organizations Use Cyberlaundering to Fund Their Activities, and How Governments are Trying to Stop Them. *Information and Communications Technology Law* 20(2), pp.133-152.

Iltalehti, 2010. "Mafiatyylinen johtamismalli" [Mafia-Style Leading Model]. *Iltalehti*. [online] Available at: <https://www.iltalehti.fi/uutiset/a/2010112812769651> [Accessed 20 May 2019]. (in Finnish).

Iltalehti, 2018. Poliisi Huomasi Ilmiön: Rikollisjengeihin Liittyy Nyt Paljon Maahanmuuttajia - Helvetin Enkelit Vahvistui Uudella Kerholla [the Police Has Noticed a New Trend: Many of the Foreigners Join the Criminal Gangs – Hell's Angels Reinforced by a New Chapter]. *Iltalehti.* [online] Available at: < https://www.iltalehti.fi/kotimaa/a/201802122200737838> [Accessed 15 June 2019]. (in Finnish).

Iltalehti, 2019. Putinin Mp-Jengi Yön Sudet Levittäytyi Suomeen - Ensimmäinen Kerho jo Toiminnassa [Putin's Night Wolves MC has arrived in Finland – Firts Chapter is Already Established]. *Iltalehti.* [onbline] Available at: <https://www.iltalehti.fi/kotimaa/a/5664d976-cf33-49dd-98b9-d189145b5d97> [Accessed 20 June 2019]. (in Finnish).

IMF, 2004. *Financial Intelligence Unit: An Overview.* Washington: International Monetary Fund. [online] Available at: < https://www.imf.org/en/Publications/Manuals-Guides/Issues/2016/12/30/Financial-Intelligence-Units-An-Overview-17369> [Accessed 13 April 2019].

International Money Laundering Network (IMOLIN), 2019. Caribbean Financial Action Task Force: 19 Aruba Recommendations. *IMOLIN.* [online] Available at: < https://www.imolin.org/imolin/cfatf19.html> [Accessed 29 June 2019].

Johnson, K. L., 1986. Making the intelligence "Cycle" work. *International Journal of Intelligence and Counterintelligence* 1(4), pp.1-23.

Jukarainen, P., and Muttilainen, V., 2015. *Rahanpesun ja Terrorismin Rahoituksen Kansallinen Riskiarvio 2015* [*ML/TF National Risk Assessment 2015*]. Tampere: Poliisiammattikorkeakoulu. [online] Available at: <https://www.theseus.fi/bitstream/handle/10024/97954/Raportteja_117_verkko.pdf?sequence=1&isAllowed=y> [Accessed 20 April 2019]. (in Finnish).

Keene, D. S., 2012. *Threat Finance: Disconnecting the Lifeline of Organised Crime and Terrorism.* Surrey: Gower Publishing Company.

Kiinteistönvälitysalan keskusliitto Ry, 2018. *Kiinteistövälitysalan Yleisohje Rahanpesun ja Terrorismin Rahoittamisen Estämiseksi Sekä Pakotteiden Noudattamiseksi* [*General Guide of Prevention of TF and Sanction Compliance for the Real Estate Sector*]. Helsinki: Kiinteistönvälitysalan Keskusliitto Ry. [online] Available at: <https://kvkl.fi/wp-content/uploads/2019/01/Rahanpesuohje_1_2_2018-kopio.pdf> [Accessed 10 July 2019]. (in Finnish).

Koivisto, P., 2017. *Talousrikostutkinta ja sen ominaispiirteet* [*Feauters of Financial Crime investigation*]. Tampere: Poliisiammattikorkeakoulu. [online] Available at: < https://www.theseus.fi/bitstream/handle/10024/132892/ON_%20Koivisto_Panu.pdf?sequence=1&isAllo wed=y> [Accessed 13 July 2019]. (in Finnish).

Kommer, V., 2013. Cash Economy, Measuring the Tax Gap from the Tax Administrative Perspective. In: B. Unger, & D. van de Linde, ed. 2013. *Research Handbook on Money Laundering*. UK/USA: Edward Elgar Publishing Limited.

Koningsveld, J., 2013. Money Laundering – "You Don't See It Until You Understand It": Rethinking the Stages of the Money Laundering Process to Make Enforcement More Effective. In: B. Unger, & D. van de Linde, ed. 2013. *Research Handbook on Money Laundering*. UK/USA: Edward Elgar Publishing Limited.

KRP, 2012. *Rahnpesun Torjunnan Parhaat Käytänteet* [*Best Practices of Money Laundering Prevention*]. Keskusrikospoliisi: Rahanpesun Selvittelykeskus. [online] Available at: <https://www.poliisi.fi/instancedata/prime_product_julkaisu/intermin/embeds/poliisiwwwstructure/26327 _Rahanpesun_torjunnan_parhaat_kaytanteet_27.8.2012.pdf?48595bdea3a3d688> [Accessed 14 April 2019].

Lake, N., 2015. Human Trafficking Money in the Community Banks. *ACAMS*. [online] Available at: < https://www.acams.org/aml-white-paper-human-trafficking-community-banks/> [Accessed 22 June 2019].

Levi, M., 2013. The Costs of Fraud. In: B. Unger, & D. van de Linde, ed. 2013. *Research Handbook on Money Laundering*. UK/USA: Edward Elgar Publishing Limited. *Crime, Law and Social Change* 69, pp.

Levi, M., Reuter, P. and Halliday, T., 2018. Can the AML System Be Evaluated Without Better Data?. *Crime, Law and Social Change* 69, pp.307-328.

Makarenko, T., 2004. The Crime-Terror Continuum: Tracing the Interplay between Transnational Organised Crime and Terrorism. *Global Crime* 6(1), pp.129-145.

Malkki, L., and Saarinen, J., 2019. *Jihadistinen Liikehdintä Suomessa [Jihadi Movements in Finland]*. Helsinki: Sisäministeriö. [online] Available at: <http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161501/SM_14_2019_%20jihadistinen%20liikehdinta%20suomessa.pdf> [Accessed 15 April].

Marat, E., 2015. Global money laundering and its domestic political consequences in Kyrgyzstan. *Central Asian Survey* 34(1), pp.46-56.

Maxwell, J. N., and Artingstall, D., 2017. *The Role of Financial Information-Sharing Partnerships in the Disruption of Crime*. London: RUSI. [online] Available at: < https://rusi.org/publication/occasional-papers/role-financial-information-sharing-partnerships-disruption-crime> [Accessed 6 June 2019].

McCarthy, J. K., 2013. Why Do Some States Tolerate Money Laundering? On the Competition for Illegal Money. In: B. Unger, & D. van de Linde, ed. 2013. *Research Handbook on Money Laundering*. UK/USA: Edward Elgar Publishing Limited.

MONEYVAL, 2015. *"De-Risking" Within Moneyval States and Territories*. Strasbourg: Council of Europe. [online] Available at: < https://www.coe.int/en/web/moneyval/implementation/de-risking> [Accessed 15 May 2019].

Morris-Cotterill, N., 1999. Use and Abuse of the Internet in Fraud and Money Laundering. *International Review of Law, Computers and Technology* 13(2), pp.211-228.

Oxford Learner's Dictionary, 2019. [online] Available at: < https://www.oxfordlearnersdictionaries.com/definition/english/effectiveness?q=effectiveness> [Accessed 24 July 2019].

Paananen, V., 2019. Supo: myös Isis-lapset voivat olla turvallisuusuhka Suomelle [the SIS: the returning Isis Children can also be a National Threat to Finland]. *Helsingin Sanomat.* [online] Available at: <https://www.hs.fi/politiikka/art-2000006153510.html> [Accessed 17 June 2019]. (in Finnish).

Paunone, R., 2018. Airiston Helmi: Törkeää rahanpesua vai vakava turvallisuusuhka? [Airiston Helmi: Aggravated Money Laundering or a National Threat?]. *Iltalehti.* [online] Available at: <https://www.iltalehti.fi/kotimaa/a/03e22119-aeea-48a4-9dbd-142a2e6faba1> [Accessed 18 May 2019]. (in Finnish).

Perrow, C., 1991. A Society of Organizations. *Theory and Society*, 15, pp.725–62.

Prezelj, I., 2014. Inter-organizational Cooperation and Coordination in the Fight against Terrorism: From Undisputable Necessity to Paradoxical Challenges. *Comparative Strategy* 33(4), pp.321-341.

Prezelj, I., 2013. Improving Inter-organizational Cooperation in Counterterrorism: Based on a quantitative SWOT assessment. *Public Management Review* 17(2), pp.209-235.

Provan, G. K., and Sydow, Jorg., 2009. Evaluating Inter-Organizational Relationships. In: S. Cropper, C. Huxham, M. Ebers, and P. Ring, ed. 2009. *The Oxford Handbook of Inter-Organizational Relations*. Oxford: Oxford University Press.

Reuter, P., and Truman, M. T., 2004. *Chasing Dirty Money: The Fight Against Money Laundering*. Washington, DC: Institute for International Economics.

Rimpiläinen, T., and Mansikkamäki, E., 2017. Tämä kaikki Turun puukkoiskusta tiedetään – historiallinen oikeudenkäynti kestää useita päiviä [All Information About Turku Terror-Attack – Historical Trial WIll Last Several Days]. *Aamulehti.* [online] Available at: <https://www.aamulehti.fi/a/200392412> [Accessed 17 June 2019]. (in Finnish).

Rudner, M., 2010. Hizbullah Terrorism Finance: Fund-Raising and Money-Laundering. *Studies in Conflict & Terrorism* 33(8), pp.700-715.

Salminen, J., and Suomala, E., 2018. *Satudarah MC:n tulevaisuus Suomessa* [*the Future of Satudarah MC in Finland*]. Tampere: Poliisiammattikorkeakoulu. [online] Available at: <https://www.theseus.fi/bitstream/handle/10024/154683/ON_Suomala_Salminen.pdf?sequence=1&isAll owed=y> [Accessed 18 July 2019]. (in Finnish).
o.fi/terrorismintorjunta/terrorismin_uhka-arvio> [Accessed 10 July 2019]. (in Finnish).

Sathye, M., 2008. Estimating the cost of compliance of AMLCTF for financial institutions in Australia. *Journal of Financial Crime* 15(4), pp.347-363.

Scott, L., and Jackson, P., 2004. The Study of Intelligence in Theory and Practice. *Intelligence and National Security* 19(2), pp.139-169.

Serio, D. J., 2004. Fueling global crime: the mechanics of money laundering. *International Review of Law, Computers & Technology* 18(3), pp.435-444.

Schott, A. P., 2006. *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism.* Washington: The International Bank for Reconstruction and Development/The World Bank/The International Monetary Fund.

Shiraz, Z., 2013. Drugs and Dirty Wars: Intelligence Cooperation in the Global South. *Third World Quarterly* 34(10), pp.1749-1766.

Siäsministeriö, 2018. *National Counter-Terrorism Strategy 2018-2021.* Helsinki: Sisäministeriö. [online] Available at: <http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161188/28_2018_National%20Counter-Terrorism%20Strategy%202018-2021_netti.pdf> [Accessed 15 July 2019].

Sisäministeriö, 2019. *Rahanpesun ja Terrorismin Rahoittamisen Torjunta* [*Anti-Money Laundering and Counter Terrorism Financing*]. Sisäministeriö. [online] Available at: < https://intermin.fi/rahanpesun-ja-terrorismin-rahoituksen-torjunta> [Accessed 20 July 2019].

Stokes, R., 2012. Virtual Money Laundering: The Case of Bitcoin and the Linden Dollar. *Information and Communications Technology Law* 21(3), pp.221-236.

Suomen Asianajajliito, 2017. *Rahanpesun ja Terrorismin Rahoittamisen Estäminen* [*Prevention of Money Laundering and Terrorist Financing*]. Helsinki: Suomen Asianajajliitto. [online] Available at: <https://asianajajaliitto.fi/asianajajaliitto/yhteiskuntavastuu/rahanpesun-ja-terrorismin-torjunta/> [Accessed 11 July 2019]. (in Finnish).

Suomen Poliisi, 2019a. *Jäörjestäytyneen Rikollisuuden Torjunta Käsikirja* [*Handbook on Prevention of Organised Crime*]. Suomen Poliisi. [online] Available at: <https://www.poliisi.fi/instancedata/prime_product_julkaisu/intermin/embeds/polisenaxwwwstructure/79346_JR-kasikirja_nettiversio.pdf?bbe1899d20b4d688> [Accessed 17 July 2019]. (in Finnish).

Suomen Poliisi, 2019. *Rahanpesun Torjunta* [*Money Laundering Prevention*]. Suomen Poliisi. [online] Available at: <https://www.poliisi.fi/rahanpesu> [Accessed 13 June 2019]. (in Finnish).

Suomen Poliisi, 2019. *Keskusrikospoliisin tehtävät* [*Tasks of the National Bureau of Investigation*]. Suomen Poliisi. [online] Available at: <https://www.poliisi.fi/keskusrikospoliisi/tietoa_krp_sta> [Accessed 12 July 2019]. (in Finnish)

Suomen Poliisi, 2019. *Organisaatio* [*Organisation*]. Suomen Poliisi. [online] Available at: <https://www.poliisi.fi/tietoa_poliisista/organisaatio> [Accessed 15 July 2019]. (in Finnish)

Suomen Poliisi, 2019. *Poliisihallitus* [*National Police Board*]. Suomen Poliisi. [online] Available at: < https://www.poliisi.fi/poliisihallitus> [Accessed 20 July 2019]. (in Finnish).

Suomen Poliisi 2017. *Poliisin Strategia 2017-2020* [*Police Strategy 2017-2020*]. Suomen Poliisi. [online] Available at: < https://www.poliisi.fi/instancedata/prime_product_julkaisu/intermin/embeds/poliisiwwwstructure/57642_POL_ST_esite_suomi_210x280_LR.pdf?1ba9169f36d0d588> [Accessed 15 July 2019]. (in Finnish)

Suomen Tilintarkastajat Ry, 2017. *Tilintarkastajan Rooli Rahanpesun ja Terrorismin Rahoittamisen Estämisessä* [*the Role of an Auditor in AML/CTF*]. Helsinki: Suomen Tilintarkastajat Ry. [online] Available at: <https://www.suomentilintarkastajat.fi/tilintarkastus/ohjeita-ja-suosituksia/tilintarkastajan-rooli-rahanpesun-ja-terrorismin-rahoittamisen-estamisessa> [Accessed 10 July 2019]. (in Finnish).

SUPO, 2018. Juhlavuosikirja 2018 [Annual Review 2018]. *Suojelupoliisi.* [online] Available at: <https://www.supo.fi/julkaisut/esitteet> [Accessed 30 May]. (in Finnish).

SUPO. 2018. *Terrorismin uhka-arvio 14.6.2017* [*Terrorist Threat Assesment 2017*]. Suojelupoliisi. [online] Available at: <https://www.supo.fi/terrorismintorjunta/terrorismin_uhka-arvio> [Accessed 10 July 2019]. (in Finnish).

SUPO, 2019. *10 Kysymystä Siviilitiedustelusta* [*10 Questions about Civilian Intelligence*]. Suojelupoliisi. [online] Available at: <https://www.supo.fi/tietoa_suposta/tiedustelulaki> [Accessed 12 July 2019]. (in Finnish).

Tang, S., 2007. A Systematic Theory of the Security Environment. *Journal of Strategic Studies* 27(1), pp.1-34.

Taylor, W. T., and Russel, L. A., 2011. To take this complex landscape into account, the proposed research should be. Formulated in a way that highlights how where. *Police, Practice and Research: an International Journal* 13(2), pp.184-200.

Thomas, J., 2019. Money Laundering and the Illegal Wildlife Trade. *The Asean Post.* [online] Available at: < https://theaseanpost.com/article/money-laundering-and-illegal-wildlife-trade> [Accessed 20 June 2019].

Treverton, F. G., 2016. *New Tools for Collaboration: The Experience of the U.S. Intelligence Community.* Center For Strategic and International Studies. [online] Available at: <https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/160111_Treverton_NewTools_Web.pdf> [Accessed 15 March].

United Nations, 1988. *United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances.* New York: UN. [online] Available at: <https://www.unodc.org/pdf/convention_1988_en.pdf> [Accessed 3 July 2019].

United Nations, 2004. *United Nations Convention Against Transnational Organized Crime and the Protocols Thereto.* New York: UN. [online] Available art: < https://www.unodc.org/documents/middleeastandnorthafrica/organised-crime/UNITED_NATIONS_CONVENTION_AGAINST_TRANSNATIONAL_ORGANIZED_CRIME_AND_THE_PROTOCOLS_THERETO.pdf> [Accessed 2 July 2019].

United Nations, 1999. *International Convention for the Suppression of the Financing of Terrorism.* New York: UN. [online] Available at: <https://www.unodc.org/documents/treaties/Special/1999%20International%20Convention%20for%20the%20Suppression%20of%20the%20Financing%20of%20Terrorism.pdf> [Accessed 2 July 2019].

United Nations, 2004. *United Nations Convention Against Corruption.* New York: UN [online] Available at: <https://www.unodc.org/documents/brussels/UN_Convention_Against_Corruption.pdf> [Accessed 1 July 2019].

United Nations Office on Drugs and Crime, 2019. Money-Laundering and Globalization. *UNODC.* [online] Available at: < https://www.unodc.org/unodc/en/money-laundering/globalization.html> [Accessed 28 March 2019].

United Nations Office on Drugs and Crime, 2011. *Estimating Illicit Financial Flows Rsulting from Drug Trafficking and Other Transnational Organized Crimes.* Vienna: UNODC. [online] Available at: < https://www.unodc.org/unodc/en/frontpage/2011/October/illicit-money_-how-much-is-out-there.html> [Accessed 17 May 2019].

United Nations Office on Drugs and Crime, 2019. Technical Assistance Against Money-Laundering. *UNODC.* [online] Available at: < https://www.unodc.org/unodc/en/money-laundering/technical-assistance.html> [Accessed 1 July 2019].

Unger, B., 2013. Money Laundering Regulation: from Al-Capone to Al Qaeda. In: B. Unger, & D. van de Linde, ed. 2013. *Research Handbook on Money Laundering.* UK/USA: Edward Elgar Publishing Limited.

United Nations Security Council, 2001. *Resolution 1373 on Threats to International Peace and Security Caused by Terrorist Acts (S/RES 1373).* UNSC. [online] Available at: <https://www.unodc.org/pdf/crime/terrorism/res_1373_english.pdf> [Accessed 3 July 2019].

United Nations Security Council, 1999. *Resolution 1267 on Afghanistan (S/RES 1276).* UNSC. [online] Available at: < http://unscr.com/en/resolutions/1267> [Accessed 3 July 2019].

United Nations Security Council, 2019. Security Council Committee pursuant to resolutions 1267 (1999) 1989 (2011) and 2253 (2015) concerning ISIL (Da'esh) Al-Qaida and associated individuals groups undertakings and entities. *UNSC.* [online] Available at: < https://www.un.org/securitycouncil/sanctions/1267> [Accessed 10 July 2019].

United Nations Security Council, 2014. *Resolution 2178 on Threats to International Peace and Security Caused by Foreign Terrorist Fighters.* UNSC. [online] Available at: <https://www.un.org/securitycouncil/s/res/2178-%282014%29> [Accessed 20 June 2019].

Utrecht University, 2013. *Project 'ECOLEF' The Economic and Legal Effectiveness of Anti- Money Laundering and Combating Terrorist Financing Policy.* Utrecht: European Commission DG Home Affairs. [online] Available at: <http://www2.econ.uu.nl/users/unger/ecolef_files/Final%20ECOLEF%20report%20(digital%20version).pdf> [Accessed 20 April 2019].

Valtioneuvosto, 2016. *Valtioneuvoston Periaatepäätös Kansalliseksi Harmaan Talouden ja Talousrikollisuuden Torjunnan Strategiaksi 2016-2020* [*Goverment Resolution on for a National Strategy for Prevention of Grey Economy and Financial Crimes 2016-2020*]. Helsinki: Valtioneuvosto. [online] Available at: <https://oikeusministerio.fi/documents/1410869/3723676/VN+periaatepäätös+harmaan+talouden+torjunta/4c2e9795-9d6f-4fe4-9be7-b96dedd48635/VN+periaatepäätös+harmaan+talouden+torjunta.pdf> [Accessed 25 April 2019]. (in Finnish).

Verohallinto, 2019. *Verohallinto taklaa veropetoksia tehokkaasti* [*Tax Office's Effective Prevention of Tax Exvasion*]. Helsinki: Verohallinto. [online] Available at: <https://www.vero.fi/harmaa-talous-rikollisuus/torjunta/verotus/> [Accessed 2 June 2019]. (in Finnish).

Vettori, B., 2013. Evaluating Anti-Money Laundering Policies: Where Are We? In: B. Unger, & D. van de Linde, ed. 2013. *Research Handbook on Money Laundering*. UK/USA: Edward Elgar Publishing Limited.

Walker, J., and Unger, B., 2013. Measuring Global Money Laundering: The Walker-Gravity Model. In: B. Unger, & D. van de Linde, ed. 2013. *Research Handbook on Money Laundering*. UK/USA: Edward Elgar Publishing Limited.

Zakarte, C. J., 2013. *Treasury's War: The Unleashing of a New Era of Financial Warfare.* New York: PublicAffairs.