Financial surveillance and the role of the Financial Intelligence Unit (FIU) in the Netherlands

Pieter Lagerwaard
Department of Political Science, University of Amsterdam, Amsterdam, The Netherlands

Abstract

Purpose – In 2019, FIU-the Netherlands celebrated its 25th anniversary. This study takes the occasion to reflect on the role of the FIU in financial surveillance and to describe its core practices of collecting, analysing and disseminating financial intelligence.

Design/methodology/approach – Because FIU practices are often secret and its transaction data classified as state secrets, the FIU's daily operational activities remain obscure. Drawing on interviews, public reports and an online training course, this study encircles secrecy and offers a fine-grained analysis of the FIU's core activities.

Findings – The article finds that the FIU plays a pivotal role in financial surveillance because it can operate at various intersections. An FIU operates at the intersection of finance and security, in between the public and private sector and at the national and international domain. This pivotal role makes the FIU indispensable in the surveillance of payment systems and spending behavior.

Social implications – The article poses that the desirability and effectiveness of financial surveillance has to date not received sufficient consideration, while it affects (the privacy of) anyone with a bank account. The article asks: is it ethically justifiable that transaction information is declared suspect, investigated, and shared nationally and internationally, without the individual or entity concerned officially being notified and legally named a suspect?

Originality/value – This case-study is not only relevant for the study of finance/security, AML/CFT and financial surveillance, but also to policy makers and the broader public who merit an understanding of how their financial behaviour is being surveilled.

Keywords Financial Intelligence Unit, Encircling secrecy, Financial surveillance, Privacy and proportionality

Paper type Research paper

The research for this paper has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation program (research project "FOLLOW: Following the Money from Transaction to Trial", Grant No. ERC-2015-CoG 682317). I would like to thank the whole FOLLOW team for the inspiring years of working together.

Journal of Money Laundering
Control
Vol. 26 No. 7, 2023
pp. 63-84
Emerald Publishing Limited
1368-5201
DOI 10.1108/JMLC-09-2022-0134

Introduction: Financial Intelligence Unit-the Netherlands

> There's a story behind every criminally-gained euro. A story that a banknote or bank transfer doesn't reveal but for some reason does end up at the FIU-the Netherlands. (Akse, 2019, p. 6)

To mark its 25th anniversary, the Financial Intelligence Unit of the Dutch police (henceforth, FIU-the Netherlands) published a book on the FIU's origins and core tasks (Akse, 2019) [1]. The book provides specific examples of the FIU's value to matters of security, for example, when a woman wanted to withdraw €100,000 in cash, to have – such was the suspicion – her ex-boyfriend murdered. Accordingly, this money was not paid out. Another well-known example is the FIU's contribution to the investigation into the murder of politician Pim Fortuyn, by Volkert van der Graaf. Based on the FIU's financial data, the police were able to trace his whereabouts and conduct a search on the day of the murder. According to the jubilee book, "intelligence on reported transactions increasingly stakes an own rightful place in investigation and prosecution [. . .]. Whether it concerns the murder of Fortuyn, payment for a container of fruit with concealed parcels of cocaine or a healthcare fraud, [. . .] reported transactions played a crucial or supportive role in all these kinds of investigations" (Akse, 2019. p. 8).

During its now more than twenty-five years of existence, the Dutch FIU has grown to become the pivot of financial surveillance in the Netherlands. Coupled with the increasing digitisation of payment services, as societies have transitioned from the use of coins and notes to digital transactions, a growing volume of financial transaction data have become available, from banks, but also from shops and payment service providers such as Western Union. These data provide a wealth of intelligence on spending behaviour of citizens and thus possibly provide an insight into criminal activities. Commercial companies such as banks that have access to transaction data are therefore often seen as "gatekeepers" of the financial system. According to the "Money Laundering and Terrorist Financing (Prevention) Act" in the Netherlands [2], these gatekeepers must monitor their customers for unusual, potentially criminal activities. Banks in the Netherlands are now estimated to have more than 12,000 employees whose primary task is to conduct customer screening, monitor funds transfers and transaction behaviour of Dutch citizens and to report unusual transactions to the FIU (Kamphuis, 2021). The FIU is the leading authority that collects all reports on unusual transactions. It examines these further and disseminates the intelligence to the relevant investigation and prosecution authorities.

Given the pivotal role played by the FIU in financial surveillance, it is remarkable how little is known about the daily operations of this relatively new organisation. There is a growing literature that focuses on the increasing use of financial data for security purposes (Amicelle, 2017b), the role of banks and technology in combating terrorist financing (Bosma, 2019) and the lawsuits arising from these security efforts (Anwar, 2020). However, little is known about the exact role that the FIU plays in the wider financial surveillance system. There are notable exceptions of studies that investigate how banks and FIUs collaborate (Amicelle, 2017a), how FIUs collaborate at a European level and the legislative framework in which this happens (respectively Lagerwaard, 2020; Mouzakiti, 2020) and how FIUs exchange intelligence at an international level (Amicelle and Chaudieu, 2018), but, as far as I know, there is no detailed study of the daily practices of a single FIU. In addition, literature on surveillance pays little attention to this form of *financial* surveillance. The FIU is neither a conventional "Orwellian" public security service because it uses private payment data (Orwell, 1949), nor is it a large private company like Google or Facebook that use their databases to monitor behaviour for commercial purposes, which Zuboff recently called "Surveillance Capitalism" (2019).

It is important to understand the operations of financial surveillance and the role of the FIU because the information that circulates concerns sensitive private information, which raises questions on privacy and proportionality. FIU data not only contain financial intelligence but a variety of other data that contextualises the transactions because a transaction, in itself, is not very informative. As Ferrari states:

> Triangulated with other personal data points, [financial transactions] allow to infer information about individuals' activities, purchases and geographical movements, from which, in turn, sexual orientation, health status, religious and political beliefs and cultural preferences can be derived. (Ferrari, 2020, p. 522)

The public debate often focuses on the collection of personal data by private companies such as Google and Facebook (van Dijck, 2014; Zuboff, 2019) or the use of artificial intelligence (Timan and Grommé, 2020). But dissemination of this financial intelligence, in which transactions form the basis of citizens' digital risk profiles, is not generally associated with privacy and proportionality (exceptions are works by Dehouck and de Goede, 2021; Mitsilegas and Vavoula, 2016; Riemslag Baas, 2021). Financial information is increasingly used by commercial companies (Westermeier, 2020), such as by so-called FinTechs: companies that primarily develop and apply financial technologies (Hendrikse *et al.*, 2018). But, the use of these data by public actors such as the FIU remains obscure. This difference is important because, as Mouzakiti argues (2020), FIUs can be held to different legal frameworks, such as the General Data Protection Regulation (GDPR) or investigative frameworks as the European Police Data Protection Directive or, in the Netherlands, the Dutch Police Data Act. Because data from millions of transactions are collected, analysed, declared suspicious and stored in databases without informing the persons or companies that carried out the transaction, a thorough understanding of financial surveillance and the role of the FIU is important: it affects (the privacy of) anyone with a bank account.

This article examines the core tasks of FIU-the Netherlands and places these in the wider financial surveillance system. It asks how the FIU, in practice, fulfils the three core tasks of collecting, analysing and disseminating (financial) information and how it operates as a crucial pivot in the wider system of financial surveillance. The study entails methodological challenges because certain activities have not been accessible for research because of the secrecy that is part and parcel to FIU operations, in particular the actual analysis process. The FIU's database is categorised as state-secret secret, which means that direct reporting may not be published. This article "encircles" this secrecy by consulting alternative sources that provide an insight into the FIU's daily operations (Bosma *et al.*, 2019; see also Bellanova and Sætnan, 2019). Important to note: the article concentrates on the FIU's daily practices, organisational processes and the dilemmas and challenges that are identified anonymously, without reporting potentially sensitive information on ongoing investigations. The "encircling" method is supplemented by document analysis and semi-structured interviews with employees at both FIU-the Netherlands and European FIUs, allowing generic sources to be empirically situated.

The next two sections discuss respectively the theoretical background of financial surveillance and the method of "encircling" secrecy. The bulk of the article comprises the three empirical sections, each dealing with a core task of the FIU: collecting, analysing and disseminating financial intelligence. In the conclusion, I formulate several points of interest that can serve as input for further research as well as a wider (political) debate on financial surveillance and the role of the FIU.

Financial surveillance

Surveillance is a broad concept, which is often applied with various nuances. Perhaps the best-known and most imaginative concept of surveillance is the Orwellian Big Brother: a state dictator who leads a centralised power and has his "thought police" keep a close eye on the behaviour of the population via television screens (Orwell, 1949, p. 2). This classic interpretation of surveillance follows a Weberian approach, in which the focus lies on the state and bureaucracy (see, for example, Dandeker, 2007, p. 40). Another imaginative concept of surveillance is the Foucauldian panopticon: the watchtower with tinted windows in the middle of a circular prison. From a position in the watchtower, the prison guard does not have to look but *possibly looks*, leading inmates to self-discipline (Foucault, 1977). In addition to these two key concepts, there are many other approaches to surveillance, such as the modern "fluid" form of surveillance in which power and responsibilities are decentralised (Bauman and Lyon, 2013) or the surveillance of technology and large digital data sets that produce "data doubles" of individuals (Haggerty and Ericson, 2000). Lyon, Haggerty and Ball claim that "interest in surveillance studies has mushroomed, generating considerable excitement about the potential for new ways to understand human behaviour" (Lyon *et al.*, 2012, p. 1).

It is surprising that a field as extensive as *financial* surveillance which is geographically widespread across more than 160 countries, each with its own national FIUs, does not occupy a substantial position in surveillance studies. Surveillance studies traditionally focuses on topics such as cameras in the public domain (Armstrong and Norris, 1999) or the surveilling role of the information state (Weller, 2012). However, lesser-known topics are also increasingly studied from the surveillance point of view, such as the use of smartphones to monitor health (Lupton, 2012) or the increasing use of aircraft passenger data used for security purposes (Bellanova, 2014; Bellanova and Duez, 2012). Financial surveillance has no prominent position in this literature, but there are some notable exceptions. In the aftermath of the 9/11 attacks, Atia identified increasing financial surveillance of Islamic groups (Atia, 2007); in Europe, Vlcek observed how terrorist financing provides legitimacy to implement financial surveillance (Vlcek, 2007, 2009); and Amicelle already argued in 2011 that we need to develop a new concept of financial surveillance – a new "political anatomy" – which includes multiple actors with heterogeneous aims (Amicelle, 2011, p. 162; see also Amicelle and Favarel-Garrigues, 2012).

Related literature, which teaches us more about this variety of actors involved, does not focus on surveillance but on the "finance-security nexus" (Boy *et al.*, 2017; de Goede, 2010; Langley, 2017; Westermeier, 2019). This literature explores the different ways in which finance and security are intertwined, such as the use of financial resources in war situations (Gilbert, 2015). This literature increasingly focuses on the use of financial transactions for security purposes (Amoore and de Goede, 2008; Boy *et al.*, 2017). Marieke de Goede speaks of a "chain of financial security", in which the financial transaction information goes through a "chain" of actors: from commercial actors such as banks who monitor payment behaviour; to the FIU, who carries out further analysis and forwards suspicious information on to the executive authorities; to eventually the courts, where a suspect can be convicted on the basis of financial intelligence (2018). The transaction information does not remain the same as it travels through the chain but is "translated" and acquires a different meaning in each professional domain (de Goede, 2018, p. 29). According to de Goede, the FIU occupies a central position in this chain, positioned between the commercial and public actors. However, "very little [. . .] is known about how FIUs handle, share and analyse unusual transaction reports" (de Goede, 2018, p. 35; see also de Goede 2017b).

This article understands financial surveillance to be a broad-based collaboration between private and public actors who systematically monitor, filter, analyze, and use transaction information in order to ascertain the spending behavior of citizens, with the objective of detecting and, if possible, prosecuting and punishing criminal misconduct. The FIU is perhaps the most important actor, the pivot, in this system because it is the only actor that operates purely at the intersection of finance and security. As a metaphor, this pivotal role can be compared to an hourglass: on the side of reporting there are 25 professional groups – not just financial ones – that have to report unusual transactions to the FIU (FIU-Nederland, 2022c). These actors send their information to the FIU, like sand flowing in an hourglass from a broad base to the core. The FIU analyses the reports and sends the intelligence back to numerous police, justice and security services, like sand flowing from the core of an hourglass back to the broad base. However: the FIU filters the intelligence, supplements it and modifies it so that it can be applied by actors further down the security chain.

What makes the FIU so interesting is that it operates as a pivot on several intersections. On the one hand, the FIU operates at the intersection of finance and the world of banking and economic transactions and on the other hand it operates in the world of security such as the police and judicial authorities. It acts as a pivot at the intersection of both private actors as it depends on private transaction data and public authorities to whom it must forward the intelligence to find security purpose. In fact, the FIU is an intersection itself, where unusual transaction information goes in and suspicious financial intelligence comes out. And finally, the FIU operates at the intersection of the national and interterminal domain, where it plays an important role by sharing intelligence with FIUs in other countries, who have to closely work together to identify and trace international money flows (Amicelle and Chaudieu, 2018). It is surprising that, given this pivotal position, the FIU's specific role in the wider financial surveillance system remains obscure, both in scientific literature and in the political and policy-related debate.

"Encircling" of secrecy

To be able to investigate the secret processes at the FIU, I make use of the method of "encircling" secrecy (Bosma *et al.*, 2019, p. 14). The FIU's data, such as actual unusual transactions, are categorised as a "state-secret secret" at the time they are entered in the FIU database. There are four categories of sensitive information at the Dutch government level: departmental confidential, state-secret confidential, state-secret secret and state-secret very secret (VIRBI, 2013). The FIU data fall into the third category – state-secret secret – which means that specific security measures apply, such as the registration of all persons to whom the information is disclosed, the signing of a nondisclosure agreement and the possession of a Certificate of No Objection (*Verklaring van geen bezwaar*) (VIRBI, 2013). This secrecy is not without reason. The information that the FIU works with is privacy sensitive and any revelation of precise investigations by the FIU or individuals whose information is retained could be harmful to the investigation and prosecution as well as to the individuals or companies. The nondisclosure agreement, in particular, makes it difficult for researchers to examine authorities such as the FIU, because without consent there is no possibility to examine the analysis processes, but with consent restricted publication of results is allowed.

There is a growing literature that studies secrecy (Birchall, 2016) and the methodological issues that come with it (Belcher and Martin, 2019; de Goede *et al.*, 2019; Dijstelbloem and Pelizza, 2019). Bosma, de Goede and Pallister-Wilkins assert that:

> [. . .] we do not consider closed doors, partial visibilities and obfuscation necessary to constitute failed research. Instead of considering what has been lost or what stays out of the picture, we ask, what does mapping the contours of secrecy and obfuscation *add* to our analysis? (2019, p. 3)

Secrets have the stature of authenticity because they are difficult to verify (Jones, 2014). This does not mean, however, that secrets must be 'revealed', because the status and meaning of a secret can be researched without knowing the actual contents. In the case of the FIU, secrecy is not an incomprehensible process, but the data analysis is a routine – and even a little boring – process. Although general knowledge of these activities is important, the secret is not an irresolvable hurdle that prevents a detailed study. The research approach for this article is not about revealing confidential information or practices, but to "encircle" the obstacle that secrecy poses in a creative methodological manner, thus obtaining a thorough understanding of financial surveillance and the FIU. According to Bosma, de Goede and Pallister-Wilkins, encircling implies:

> [. . .] a lateral, multipronged, creative, iterative approach to secret sites, confidential materials and classified practices. It is less focused on uncovering the kernel of the secret, than it is on analysing the mundane lifeworlds of security practices and practitioners. (2019, p. 14)

As part of my research on the analyses processes of the FIU, I completed the operational analysis e-learning course offered by the International Centre for Asset Recovery of the Basel Institute on Governance [3]. This course is intended for FIU analysts and aims, among other things, to conduct the core tasks of an FIU analyst, to analyse the risks of suspicious transaction reports, to collect information from open and closed sources and to disseminate findings. This course, which mainly informs the empirical section on analysing the data, is specifically *not* about the analysis practices of FIU-the Netherlands. However, by using up-to-date details from the annual reports of FIU-the Netherlands, which are publicly accessible [4], I use the generic course to understand the specific case of FIU-the Netherlands. In addition, this article's data are based on five semi-structured interviews with employees at FIU-the Netherlands and eight interviews with FIU employees from European FIUs. To safeguard the anonymity of respondents, no direct quotes or references will be used in this article. The triangulation between these three sources makes it possible, in an ethical manner, to encircle the secrecy, to examine the core tasks of the FIU and to address important issues such as privacy, proportionality and accountability that – hopefully – will inform a broader political and academic debate.

The next three sections discuss the core tasks of the FIU, which, in practice, partially overlap because the transaction information goes through the chain and gradually modifies and "translates" in understanding (de Goede, 2018; see also Latour, 1999). These empirical sections discuss the collection of unusual transactions by commercial actors, the analysis of this data through analysis and research and the dissemination of suspicious intelligence to domestic and foreign investigation and prosecution authorities. Each section concludes with raising a number of issues, which will be further addressed in the conclusion.

Collection of transaction information

The collection of transaction information is the foundation on which the FIU, as well as the wider financial surveillance system, functions. Without this information, the FIU cannot provide any additional contribution to the investigation and prosecution services. Since the inception of the FIU's predecessor in 1994 of the Office for the Disclosure of Unusual Translations *(Meldpunt Ongebruikelijke Transacties)*, the number of reported transactions has increased substantially: from 16,215 unusual transactions in 1995, of which 2,218 were deemed to be suspicious, to 722,247 in 2020, of which 103,947 were declared suspicious. Every 24 hour, the FIU receives about 1,200–1,400 reports that are stored in a transaction database containing an average of 1.2–1.4 million unusual transactions (Akse, pp. 5–8). Who sends this transaction information to the FIU? On the basis of which grounds are the selected transactions reported? How are they submitted and stored?

The FIU receives transaction information from various reporting groups, who are often referred to in the media as the "gatekeepers" of the financial system. These reporting groups do not only consist of banks. It is also mandatory for many other professional groups that have certain access to transaction data and payment services, to report unusual spending behaviour and transaction patterns to the FIU pursuant to the Dutch Money Laundering and Terrorist Financing (Prevention) Act [*Wet ter voorkoming van witwassen en financieren van terrorisme,* (*Wwft*)]. They are deemed to be responsible for detecting – not always financial – crimes, such as corruption, drug-related activities, trafficking in human beings and smuggling, fraud, health-care fraud, misuse of virtual assets, money laundering, terrorist financing and other forms of crime (FIU-Nederland, 2020, p. 10). There are 25 professional reporting groups, including accountants, lawyers, investment firms, cryptocurrency traders, intermediaries, payment service providers, tax consultants, legal service providers, casinos, brokers, sellers of luxury goods such as gold dealers, car dealers, boat sellers and, since recently, art dealers (FIU-Nederland, 2020. p. 50; also FIU-Nederland, 2022a). It can be said that financial surveillance and combating financial crime have been woven into the very fabric of the economy.

The millions of unusual transactions that reporting groups submit do not only contain financial information but also supplementary information to place it in a broader context. The initial unusual transaction report from the reporting entity must include the following information based on the *Wwft*:

> (a) "the identity of the client, the identity of the ultimate beneficial owners [. . .];
>
> (b) the nature and number of the client's identity document [. . .];
>
> (c) the nature, time and place of the transaction;
>
> (d) the amount as well as the destination and origin of the funds [. . .];
>
> (e) the circumstances under which the transaction is deemed to be unusual;
>
> (f) a description of the particular valuable items in a transaction above €10,000; and
>
> (g) additional details, designated by order in council."
>
> - Ministry of Justice, Netherlands, 2008, sec. 16, 2

In other words, when reporting an unusual transaction the actual financial transaction only forms the basis for a broader context and a (digital) profile of the individual or company that undertook the transaction. Points a. to d. cover the general "absolute" data, such as the client's identity document [5], the nature and time of the transaction and the amount. Point g. means that the FIU can submit an inquiry to the reporting entity for additional information.

Points e. and f. require further explanation because these points highlight two different features of financial surveillance that are essential to understand the entire process of collection, analysis and dissemination. Reporting groups, including those in other countries, must report a transaction based on *objective* or *subjective* indicators. Point f. is an example of an objective indicator. This point describes that any transaction with a value greater than €10,000 must imperatively be investigated. In the case of banks for example, certain transactions such as cash deposits of this size, must be reported (FIU-Nederland, 2022b). When the "threshold" is adjusted upwards or downwards, it automatically causes an increase or decrease in the number of reports of unusual transactions at the FIU. Another objective indicator is the assessment of risk countries, as designated by the European Commission (2016) or the Financial Action Task Force [6], which marks all transactions that take place with these countries as being unusual and must be reported at the FIU. The objectivity of objective indicators is therefore not so much in the indicator itself – these are based on certain assumptions – but derives from the fact that it can be implemented "objectively" in the often automatic monitoring systems.

The subjective indicator, in contrast, calls on a reporting entity to consider the risk of a transaction, based on personal, normative assumptions of a customer's payment behaviour. Point e. is an example of this, because it requires the reporting entity to describe the circumstances that classify the transaction as unusual. The Tax and Customs Administration in the Netherlands interprets this point as "why do you find the transaction to be unusual?" (Belastingdienst, 2022). While the FIU prescribes five objective indicators for banks, there is only one description in the case of the subjective indicator: "A transaction for which the institution has reason to believe that it may be related to money laundering or terrorist financing" (FIU-Nederland, 2022b). This subjective indicator is open to interpretation and relies on the commercial reporting person's ability to recognise a crime or financial criminality. Regulators for certain sectors provide guidelines for subjective indicators, such as the Dutch Authority for the Financial Markets (AFM, 2020) and De Nederlandse Bank (DNB, 2020), but these are not policy rules and are not legally binding. In this context, it is the normative suppositions of commercial operators that to a considerable extent form the "front line" of financial surveillance by providing the information on which the chain of financial security and the combating of financial crime, is vested (de Goede, 2017a).

The number of reported unusual transactions has risen significantly over the past decade, as shown in Figure 1. Reporting groups submit their reports via a reporting form or XML Report [7]. The reporting form is often used by minor reporting entities of luxury goods, who do not report very often (FIU-Nederland, 2022a). XML Reports are used by major reporting entities such as banks, who automate their reporting systems by harmonising the XML – eXtensible Markup Language – to the FIU's XML. The capacity reporting groups invest and the number of reports they submit varies considerably. For example, in 2020, casino's reported 3,764 unusual transactions while banks reported 245,148 unusual transactions. An important observation about Figure 1 and these statistics is that the substantial growth in 2019 mainly results from a reinterpretation of the risk countries. This

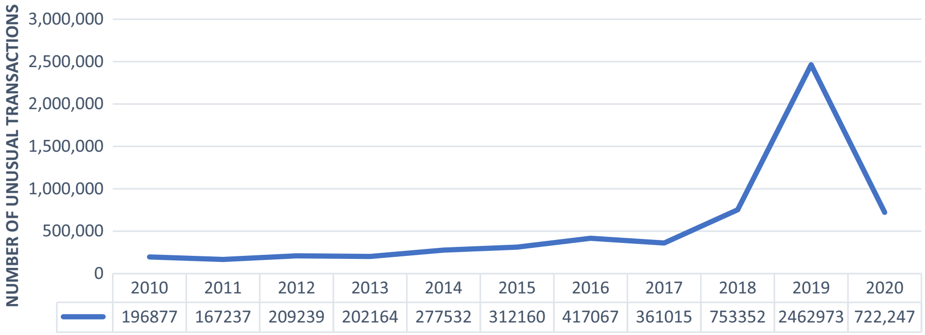


Figure 1. Longitudinal overview of the number of unusual transactions at FIU-the Netherlands

Source: This figure is based on previous fieldwork (Lagerwaard, 2018), and information from the annual reports of the FIU (FIU-Nederland, 2019, 2020, 2021) objective indicator was responsible for as much as 1,921,737 unusual transaction reports in 2019 (FIU-Nederland, 2020, p. 31). To reduce this kind of reporting, this objective indicator was changed to a subjective indicator in 2020, which means that reporting entities must now assess and decide for themselves what a risk country exactly is (FIU-Nederland, 2020). The number of reports, therefore, does not directly reflect an actual increase in unusual financial behaviour in society, but shows that the frameworks of and compliance with the indicators largely determine the increase or decrease in the number of unusual transaction reports.

In view of the substantial number of unusual transactions received by the FIU from the 25 reporting groups in the Netherlands – as the complement of employees involved in such reporting at banks alone numbers more than 12,000 (Kamphuis, 2021) – the FIU might be expected to have a large staff as well. However, the FIU is a relatively small organisation with a workforce of 76 employees in 2020 (FIU-Nederland, 2021, p. 16). The financial capacity is also relatively small compared to banks. In recent years, the major banks in the Netherlands have invested billions – ABN Amro alone has invested more than one billion euros (a thousand million) by 2021 and is planning on investing another billion (de Boer, 2021). The FIU, on the other hand, has an annual budget of €9mn (FIU-Nederland, 2021, p. 16). These ratios raise the question of proportionality: is the input from the reporting groups in proportion to the effectiveness of the FIU? Moreover, these ratios broach a practical dilemma. Given the millions of unusual transactions reported and the limited human and financial capacity of the FIU, the FIU's task would seem overwhelming. How does FIU-the Netherlands analyze the unusual transactions reported to it, as these number more than a thousand every day?

Analysing the data

> FIU-the Netherlands' unusual transactions database is full of transactions that could imply money laundering or other forms of criminality. With the current capacity at FIU-the Netherlands and also the capacity at investigative authorities, it is not possible and neither is it desirable for that matter, to conduct an equally thorough investigation of all transactions. FIU-the Netherlands has developed a strategic control and tactical selection model, which, as far as possible, enables the correct issues to be investigated, which is also in line with the priorities of the acquiring investigation partners. (FIU-Nederland, 2020, p. 59)

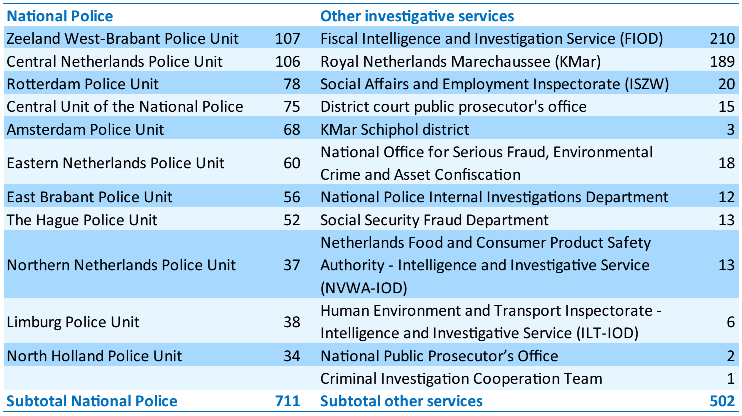
This section discusses the process from the moment the unusual transaction information is reported, until the financial intelligence leaves the FIU. This process is explicitly not linear – transactions are reported, examined, declared suspicious or not, and forwarded – but rather *source-based*, in which the entire database of unusual transactions, also known as the "buffer" between reporting and investigation (Akse, 2019, p. 38; FIU-Nederland, 2020, p. 55), forms the basis. The unusual transactions database (having 1.2–1.4 million reports) is updated every day with new reports that are stored for five years (FIU-Nederland, 2022f). This database is therefore not so much a static storage place where information is retained and digitally stored until it is destroyed but an active source of information that continuously changes. Given the capacity ratio between the reporting groups and the FIU, this source-based strategy is essential because it makes it possible not to subject all reported unusual transactions to follow-up investigations, but to routinely perform searches of the entire database based on new external research data and queries. On what grounds is an unusual transaction declared suspicious? What type of analysis investigation does the FIU itself perform? How is transaction information transformed to financial intelligence? This section first looks at how an unusual transaction can be declared suspicious, after which it describes the analysis methods of the FIU by drawing on the operational analysis course.

Declared as suspicious

A typical feature of the Dutch financial surveillance system is the distinction between unusual and suspicious transactions, in which the reported transaction in first instance is unusual and can be only declared suspicious by the FIU. The methods of filtering suspicious transactions from the unusual transaction database can be roughly divided into two groups: the semi-automated methods – often referred to as *analysis* – and the manual methods – often referred to as *investigation*.

The semi-automatic methods link the database of unusual transactions to external information sources, such as sanctions lists, databases and other data files. The most important national database that is interfaced is the Index of Criminal Investigations and Subjects – *Verwijzingsindex Recherche Onderzoeken en Subjecten* (VROS) –, which is a national police force database containing "criminal intelligence unit subjects and subjects under investigation by detectives" (KLPD, 2008, p. 174); see also FIU-Nederland, 2019, p. 23]. In 2020, 42,367 transactions were declared suspicious because the FIU database matched with the index of criminal investigations and subjects/*VROS*, representing more than one-third of the total number of suspicious transactions in that year (FIU-Nederland, 2021, p. 10). In addition, the database is regularly compared to national database files at the Prosecution Service Criminal Assets Deprivation Bureau (*Bureau Ontnemingen Openbaar Ministerie*) (KLPD, 2008, p. 174), the Central Fine Collection Agency (FIU-Nederland, 2020, p. 38) and the National Sanctions List of Terrorism (FIU-Nederland, 2020. p. 42). Foreign national sanctions lists and international lists such as those of the European Commission are also compared (FIU-Nederland, 2020), and the database is made available indirectly and anonymously to FIU.net, the system with which the European FIUs exchange data [9]. Comparisons with this host of lists, databases, and links to other data files are semi-automatic, as the information sources automatically track down suspicious transactions from *within* the database, without having to perform specific queries.

Manual methods, on the other hand, require external input for targeted searches for information in the database. These requests come primarily from the National Public Prosecutor (*LOvJ*), who is charged with this task as an intermediary for the investigation and prosecution authorities. Based on these requests for information, the FIU consults the database, declares the matching unusual transaction as suspicious and, after possibly



National Police		Other investigative services	
Zeeland West-Brabant Police Unit	107	Fiscal Intelligence and Investigation Service (FIOD)	210
Central Netherlands Police Unit	106	Royal Netherlands Marechaussee (KMar)	189
Rotterdam Police Unit	78	Social Affairs and Employment Inspectorate (ISZW)	20
Central Unit of the National Police	75	District court public prosecutor's office	15
Amsterdam Police Unit	68	KMar Schiphol district	3
Eastern Netherlands Police Unit	60	National Office for Serious Fraud, Environmental Crime and Asset Confiscation	18
East Brabant Police Unit	56	National Police Internal Investigations Department	12
The Hague Police Unit	52	Social Security Fraud Department	13
Northern Netherlands Police Unit	37	Netherlands Food and Consumer Product Safety Authority - Intelligence and Investigative Service (NVWA-IOD)	13
Limburg Police Unit	38	Human Environment and Transport Inspectorate - Intelligence and Investigative Service (ILT-IOD)	6
North Holland Police Unit	34	National Public Prosecutor's Office	2
		Criminal Investigation Cooperation Team	1
Subtotal National Police	**711**	**Subtotal other services**	**502**

Source: FIU-Nederland (2021, p. 35)

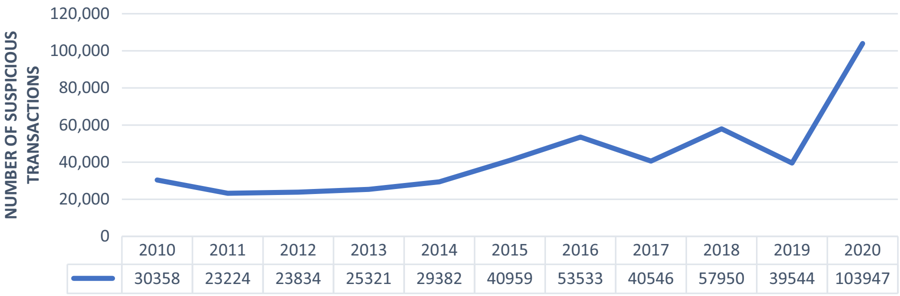
Figure 2.
National public prosecutor requests per investigation or prosecution authority in 2020

conducting further investigation, provides the intelligence (Audit Magazine, 2019, p. 21). In 2020, the FIU received 1,213 *LOvJ* requests from 23 different organisations, as shown in Figure 2. Another important manual method is the exchange of information with foreign FIUs. The *LOvJ* may request FIU-the Netherlands to apply for information from a foreign FIU and foreign FIUs may submit requests to FIU-the Netherlands (FIU-Nederland, 2020, p. 32). In 2020, FIU-the Netherlands received 650 requests for information from 77 foreign FIUs and FIU-the Netherlands itself submitted 590 requests to 85 foreign FIUs (FIU-Nederland, 2021, p. 7). This exchange can take place through what is known as diagonal cooperation, in which FIU-the Netherlands act as a mailbox that forwards information to national investigation or prosecution services (Amicelle and Chaudieu, 2018, p. 652; European Commission, 2017, p. 4). As the *LOvJ*'s requests are increasingly becoming more complex in nature, the FIU-the Netherlands intends to semi-automate these manual methods in the future as well (FIU-Nederland, 2020, pp. 6 and 9).

The suspicious transactions, in sum, derive from the active monitoring, filtering and searching of the entire unusual transactions database. As a result, intensified use of semi-automatic or manual methods can lead to an increase in suspicious transactions, which may be disproportionate to the growth or decline of unusual transactions. For instance, even though the number of *unusual* transactions in 2020 has declined, the number of *suspicious* transactions has increased considerably, as shown in Figure 3. Eventually, the selected unusual transactions are officially declared suspicious by the Head of the FIU (FIU-Nederland, 2020, p. 54), after which the reporting entity receives an automatic "confirmation of receipt" that the unusual transaction has been declared suspicious (FIU-Nederland, 2022f). The individual or company that undertook the transaction is not notified.

Analysis process

FIU-the Netherlands makes the suspicious transactions widely available to investigative services – which will be dealt with in the next section – but it also performs its own supplementary analysis. Suspicious transactions that are mutually associated are merged into files, such as the 103,947 suspicious transactions in 2020 that were merged into 19,114 files (FIU-Nederland, 2021, p. 7), about five transactions per file. In practice, the size of a file depends on the topic, the investigative capacity and the importance of the intelligence for the investigating agents further down the chain. A file may contain one or even thousands of transactions (FIU-Nederland, 2021, p. 10). Because of the FIU's limited investigative



	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
▬	30358	23224	23834	25321	29382	40959	53533	40546	57950	39544	103947

Source: This figure is based on previous fieldwork (Lagerwaard, 2018), and information from the annual reports of the FIU (FIU-Nederland, 2019, 2020, 2021)

Figure 3. Longitudinal overview of the number of suspicious transactions at FIU-the Netherlands

capacity, it selects each year a number of topical themes, such as trafficking in human beings, drug trafficking and "gaining insight into healthcare fraud" (FIU-Nederland, 2020, pp. 33–35). Policy priorities are defined by an FIU administrative body, known as the strategic steering committee, and a body to which proposals for investigations can be submitted, the tactical selection committee, which assesses proposals and determines the required capacity (FIU-Nederland, 2020. p. 60).

According to the operational analysis course, an FIU analysis consists of an "intelligence cycle", which covers seven steps: planning, collecting, evaluating, collating, analysing, reporting and disseminating. The first step, planning, concerns the selection of suspicious transactions that are investigated further, which, in the case of FIU-the Netherlands, is largely determined by the tactical selection committee. The second step, collecting, focuses on the collection of supplemental information. The course emphasises that this depends on the investigative capabilities of an FIU in legal terms and on what resources it has access to. The collection of sources follows several steps that can be visualised as a pyramid, as shown in Figure 4, and starts with the information that a reporting entity has submitted. The FIU then consults its own information by drawing on previous investigative experience and knowledge. In the case of FIU-the Netherlands, for example, the selected themes by the strategic steering committee result in an accumulation of knowledge on certain topics, that can be consulted during investigations.

At the bottom of the pyramid are national and international open and closed sources. FIU-the Netherlands consults several closed national sources, such as Infobox Criminals and Inexplicable Assets (FIU-Nederland, 2020, p. 33), tax data (which can be requested) (FIU-Nederland, 2020. p. 59) and the police systems to which the FIU is connected. Closed international sources – according to the course – are derived from cooperation with foreign organisations such as Europol, Interpol or foreign FIUs. In particular, FIUs have committed

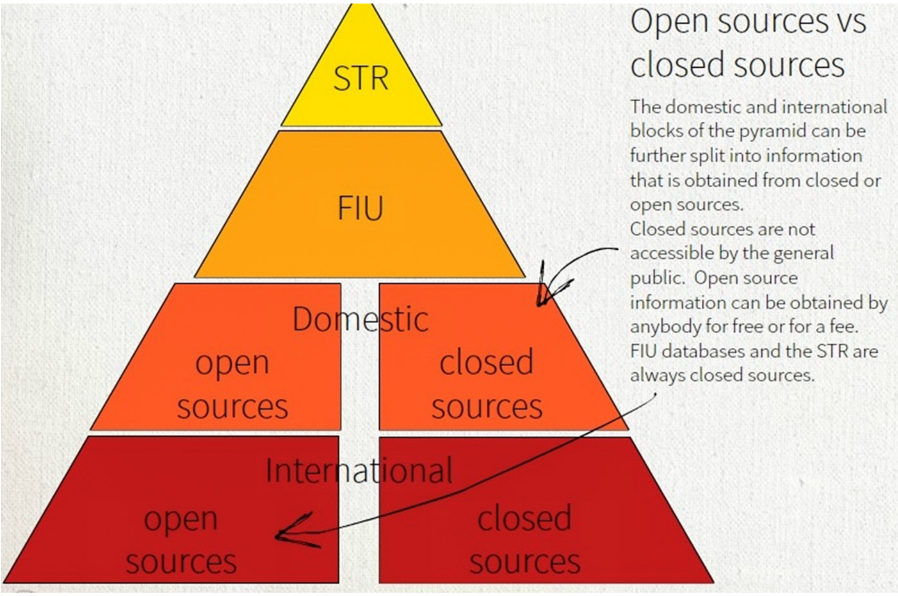

STR
FIU
Domestic
open sources
closed sources
International
open sources
closed sources
Open sources vs closed sources
The domestic and international blocks of the pyramid can be further split into information that is obtained from closed or open sources.
Closed sources are not accessible by the general public. Open source information can be obtained by anybody for free or for a fee.
FIU databases and the STR are always closed sources.

Figure 4.
Collection of open and closed sources

Source: Reproduced from basel institute on governance (2017) to freely share as much intelligence as possible, including their own closed sources (Egmont Group, 2013, 2017). Open sources may include publicly available information, such as the commercial register of the Chamber of Commerce, but also the variety of information accessible via the internet: Google search results, annual reports of organizations, company websites, journalistic articles and programs, scientific research and social media, such as Facebook, Twitter, and Instagram. FIU-the Netherlands makes use of open source intelligence and developed special software in 2019 to make "open sources more easily available and to train researchers in this" (FIU-Nederland, 2020, p. 14). The third step of the intelligence cycle, evaluating, comprises an assessment of the reliability and validity of the found information and step four, collation, the arranging of the information in preparation for the analysis.

Step five, analysis, comprises several elements: a thorough study of the sources, the formulation of a hypothesis, conducting further research and ultimately the formulation of a substantiated argument. According to the course, numerous analytical methods provide support, such as the use of an association matrix, in which sources are connected and their correlation is determined, or a link chart, in which information and its correlation can be visualised. FIU-the Netherlands works with different methods of analysis. For example, FIU-the Netherlands states that "by using a high-performance reporting and analysis tool", it produces targeted reports and analyses, with which "FIU-the Netherlands tries to identify so-called red flags through qualitative research, which can filter precisely those transactions from the database that are linked to a certain type of crime" (FIU-Nederland, 2020, p. 59). From the case studies released by FIU-the Netherlands, it can be concluded that different analysis methods are used. For example, the FIU applied "network analysis" for an investigation into cross-border flows of funding (FIU-Nederland, 2020. p. 17), carried out "transaction analyses" on drug and letting offences (FIU-Nederland, 2020. p. 18) and criminal organisations (Akse, 2019, p. 73) and it produces "financial profiles" of trafficking in human beings (Akse, 2019. p. 60), illegal exchange practices (FIU-Nederland, 2020, p. 27) or terrorist financing (FIU-Nederland, 2020. p. 43).

According to the course, during the analysis process a transformation takes place from simple financial information to financial intelligence. It defines information as the "raw data" and "the knowledge communicated or received concerning some fact or circumstance" (Basel Institute on Governance, 2017). Intelligence, on the other hand, consists of the inference of this information, supplemented by analysis and arguments that give meaning to the information. The course defines intelligence as a "value-added product derived from the collection and processing of all relevant information relating to the end user's needs, which is immediately or potentially significant to the end user's decision-making process" (Basel Institute on Governance, 2017). FIU-the Netherlands is not merely an intermediary of information from private parties to public authorities, but influences and mediates certain information, analyses, filters and investigates transactions, provides them with more information, combines them, forms arguments and merges the results into files to forward it as intelligence. Steps six and seven of the intelligence cycle, respectively, focus on the reporting and disseminating of financial intelligence, the subject of the next section.

In sum, the source-based approach offers a solution to the unbalanced ratio between millions of unusual transactions reported by the plethora of reporting groups and the FIU which has only limited capacity to examine these. The time limit of five years of storage in the database is important, because the source-based approach does not work when data are stored for a month, or would immediately be destroyed if they were deemed to be inapplicable. However, the source-based approach raises a number of issues concerning privacy and proportionality. Because unusual transactions are selected by commercial actors without intervention by for instance the public prosecutor or investigating judge, this is actually a large-scale database of information on citizens who are not officially suspect – a database of “non-suspects”. Individuals or companies from whom the – not only financial – information has been derived, are not informed that their data are incorporated in the database. Moreover, the *Wwft* and the FIU have no processes whereby individuals or entities may opt to be informed of whether their personal data appear in this database. By retaining information of millions of private transactions of non-suspects for five years, the question of proportionality arises: is the systematic collection and storage of private data of non-suspects in proportion to the security revenues? This question becomes increasingly pressing when the unusual transaction information is copied and stored in the dedicated database of only *suspicious* transactions – which is actively disseminated among investigation and prosecution authorities and with foreign FIUs around the globe.

Dissemination of intelligence

> Investigative services that acquire the most FIU information are the National Police and the FIOD [Fiscal Intelligence and Investigation Service]. FIU-the Netherlands commits to both widespread and targeted dissemination of FIU intelligence through an application to which virtually the entire police force has access. FIU-the Netherlands targets dissemination by making arrangements with those customers who acquire the information. (FIU-Nederland, 2020, p. 59)

This section examines how FIU-the Netherlands markets financial intelligence. The FIU cannot take action on its own accord because it is not authorised to apprehend or prosecute suspects. The FIU is the pivot in financial surveillance that operates on various intersections, which must bridge the gap between those reporting and those investigating, but does not have any police powers itself. The pivotal position is possible because of its exceptional institutional embedding: on the one hand, reporting groups can report their unusual transactions without being submitting directly to the police, while on the other hand, the FIU is embedded operationally in the police force. FIU-the Netherlands is a so-called “hybrid FIU” that is delegated to the police but falls under the responsibility of the Minister for Justice (Akse, 2019, p. 38). The *Wwft* highlights this hybrid position [10]. The Minister for Justice is responsible for the general management, the Minister of Finance is responsible for the budget and the head of the FIU – the director – is appointed by agreement between both ministers. In practice, the hybridity becomes even more versatile as, at an organisational level, the FIU is an independent organisation embedded in the police (Akse, 2019, p. 44; FIU-Nederland, 2020, p. 54) and adheres to for example the Police Data Act (*Wet politiegegevens*). Although the FIU is not a police authority *pur sang*, then, it does have access to the police systems and networks and is able to disseminate its intelligence via these infrastructures (Akse, 2019, pp. 35 and 38). How and to which actors does the FIU make the suspicious transactions database available? How does the FIU actively contribute to investigations and follow-up initiatives? How is the intelligence ultimately used?

There are two different types of dissemination: by either making the database of suspicious transactions available to third parties and by actively collaborating with those public authorities that are interested in financial intelligence. Similar to the unusual transaction database, analysis of the suspicious transactions database also does not follow a linear process – the intelligence is sent, investigated further and might result in a ruling – but it is also source-based. All unusual transactions that are declared suspicious by the Head of the FIU will be copied into a separate database of only suspicious transactions, containing 438,240 transactions in 2020. Transactions belonging to files which were eventually deemed to be not suspicious after further investigation by the FIU – 1,645 of the 5,302 files in 2019, with an unknown number of transactions – are also included in this database (FIU-

Nederland, 2020, p. 38). The suspicious transactions are not retained for five years but for ten years, so the database covers a broader time frame than the database of unusual transactions. In addition, these suspicious transactions are more informative than unusual ones, because they are connected to files and could be supplemented with additional intelligence from open and closed sources.

Unlike the database of unusual transactions, which is in the FIU's protected possession and is only accessible to FIU employees, the database of suspicious transactions is made available externally (Akse, 2019, p. 38). The data are made available via BlueView, a police system that was comprehensively introduced in 2007 in the Netherlands and is accessible to all investigative authorities (FIU-Nederland, 2022f). The BlueView system includes:

> [. . .] all records in the Netherlands of official reports reported to the police, of hearings, official reports, files, reports and documents relating to confiscated goods [. . .], as long as they are not older than five years. (AG connect, 2008)

The BlueView system has been typified by news media as a way to "Google" criminals (Nu.nl, 2007). By making the database of suspicious transactions available through BlueView, "old" data can appear useful only after many years, based on new investigation and intelligence facts. The database of suspicious transaction is accessible on a national scale for investigative services in the Netherlands, such as the police, special intelligence agencies, intelligence services, security services, the Public Prosecution Service, the National Office for Serious Fraud, Environmental Crime and Asset Confiscation and the 10 Regional Information and Expertise Centres [11].

The second way in which FIU-the Netherlands disseminates financial intelligence is through active collaboration with public organisations, both bilaterally and multilaterally. At a bilateral level, there is direct collaboration on some files, particularly on files which the FIU has designated a status of "suspicious embargo". In 2020, there were 65 files of this kind, involving a total of 1,725 transactions (FIU-Nederland, 2021, p. 34), which were "included in detective work, intelligence gathering and security investigations which, in connection with strict confidentiality, were only shared with the service or services involved in the investigation"(FIU-Nederland, 2020, p. 38). In addition, the FIU has several "main customers" such as the National Police and FIOD, who not only make use of the database and *LOvJ* requests but also have targeted ways of collaborating in which the FIU shares "broader views" and "specialist knowledge", also with regional police units (FIU-Nederland, 2020. p. 18). The FIU might also collaborate with a partner based on the type of crime, for example in the case of terrorist financing with the General Intelligence and Security Service and the Military Intelligence and Security Service. Or, in the case of trafficking in human beings and health-care fraud, with the Social Affairs and Employment Inspectorate (FIU-Nederland, 2020. p. 20), with whom it also worked in 2020 on a "health-care fraud monitor" (FIU-Nederland, 2020. p. 35).

FIU-the Netherlands also participates in several public–private, or public–public partnerships (PPPs), in which a variety of public and/or private parties are involved in combating a particular issue. For example, at the national level, the FIU is part of the Financial Expertise Centre, Serious Crime Taskforce, Fintell Alliance (FIU-Nederland, 2020, p. 19), Terrorist Financing Taskforce (DNB, 2019), Financial Intelligence Centre (FIU-Nederland, 2020, p. 20), and the interdepartmental working group Freezing Consultation (FIU-Nederland, 2020, p. 42). Furthermore, at the international level, the FIU is part of the Europol Financial Intelligence PPP, the Egmont Group of FIUs and the EU–FIU Platform. The FIU contributes to these collaborations not only with its own expertise or the database of suspicious transactions – to which certain other actors also have access – but because it has sole access to the database of unusual transactions. In these collaborations, banks can pass on unusual transactions that the FIU can declare suspicious, therefore making them accessible for the investigation and prosecution services via the suspicious transactions database (FIU-Nederland, 2020. p. 45). In this way, the three core tasks of FIUs combine in practice.

Despite these different forms of intelligence dissemination, it is difficult to procure an estimate of the scope in which financial intelligence is actually deployed by the investigative and prosecution services. To my knowledge, there is no quantitative data available on how financial intelligence is eventually used for investigation and prosecution. In the annual reports of the FIU and on its website, the FIU offers casuistry of for example COVID-19 benefit fraud, strategy for a "rogue letting agency", the financing of terrorism, money laundering, tax evasion and health-care fraud, in which the intelligence of the FIU was important (FIU-Nederland, 2022d). However, this intelligence is anecdotal and both for money laundering and terrorist financing – the two core tasks according to the *Wwft* – it is estimated that the eventual number of resultant lawsuits is only a couple of dozen. Between 2015 and 2020, there were about 20 terrorist financing cases [12]; yet, it is unclear how many of these cases originated from the FIU's suspicious transactions. There are, furthermore, no details known regarding the quantity of money laundering cases. In the media, an employee at the National Office for Serious Fraud, Environmental Crime and Asset Confiscation reported in 2020 that it "certainly involves a couple of dozen investigations over the past few years" (Nadrous, 2020). An important reason for the unclear and seemingly few proceeds for prosecutions is that the financial intelligence of ongoing investigations is often only a minor part of a criminal investigation, perhaps even a single pixel. As no quantitative data are maintained on this, the practical application and added value of financial intelligence – the step after dissemination – is difficult to estimate. The scope of dissemination is worthwhile for academic follow-up research.

In contrast to the unusual transactions database, the suspicious transactions database is not only accessible to FIU employees. The issue of privacy is even more prominent than in the case of the unusual transactions database, because private information on non-suspects is not only stored and analysed without knowledge and consent, it is also shared with a multitude of prosecution and investigative authorities and foreign FIUs. Again, there is no intervention by the public prosecutor or investigating judge, which means that although transactions in this database are called "suspicious", in legal terms the individuals and companies in the database are not suspect. According to the FIU's guidelines for reporting groups, the *Wwft* provides the legal basis for the agency's processing of personal data without permission, without infringing on the requirements of the General Data Protection Regulation (GDPR) (FIU-Nederland, 2022e). However, as Mouzakiti notes (2020, p. 23), different legal frameworks are at odds, as it remains unclear exactly what data protection the financial intelligence should adhere to. This is particularly significant in the international context, where, in 2020, the FIU exchanged intelligence with 85 foreign FIUs operating in different political, institutional and constitutional contexts. Is it necessary that private information of non-suspects is made available nationally and internationally? Are the unclear security revenues in combating financial crime in proportion to the impact on personal privacy?

Conclusion

In the Netherlands, financial surveillance has in recent decades grown into a widespread system that is woven into the very fabric of the economy. Increasingly, payment transactions and spending behaviour have become a source of data for investigative and prosecution services to investigate and, if possible, to contribute to the prosecution of criminal behaviour. FIU-the Netherlands is a crucial pivot in this system because this relatively new organisation operates between private and public actors. On the one hand, it depends on commercial data that forms the reservoir for the databases, and on the other hand, it depends on the public services who use the intelligence. Like the sand that flows to the core of an hourglass, the FIU receives millions of unusual transactions from 25 reporting groups, which are categorised as state-secret secret and assemble in the database of unusual transactions. By means of semi-automatic analysis and manual investigation, the FIU selects the *suspicious* transactions, after which additional analysis can be carried out using open and closed sources and analysis methods. Like the sand flowing into the broad base of the hourglass, the FIU disseminates its intelligence on suspicious transactions to a motley collection of "customers" (FIU-Nederland, 2020, p. 59). This process does not happen without modification; the FIU actively mediates the transaction information and disseminates the intelligence by not only making the suspicious transactions database available through BlueView to investigation and prosecution authorities, but also by actively entering bilateral relations and participating in multilateral and international collaborations.

In the study of surveillance, not much attention is paid to this form of *financial* surveillance. While financial surveillance is not classic Orwellian surveillance, because it is based on private, commercial data (Orwell, 1949), the FIU is a public authority that disseminates intelligence to many public investigation authorities. Financial surveillance illustrates that data collection and monitoring need not be focused on certain individuals, but neither on everyone in a population. The indicators steer the data collection in a certain direction, like control buttons that can be turned and tuned, but they do not constitute an all-encompassing "dragnet". In addition, financial surveillance shows that monitoring can take place based on intensive collaboration between public and private parties. It is a "fluid" collaboration in the sense that it explores new avenues in which data roams freely in various forms through the chain of actors (Bauman and Lyon, 2013) and is "translated" in understanding (de Goede, 2018; Latour, 1999). As a legal and operational buffer, the FIU is indispensable in this chain of actors because it operates as a pivot at the intersection of finance and security, public and private, national and international, and it is the only organisation that can convert "raw" transaction information into financial intelligence.

Societies' transition from cash spending to digital transactions makes spending behavior transparent and financial surveillance possible. Yet the questions of to what extent and in what ways this form of surveillance is feasible have received scant consideration, though these questions are increasingly pressing with the expansion of financial surveillance. To what extent is it ethically justifiable that financial intelligence concerning an individual or entity is declared suspect, investigated, and shared nationally and internationally, without the entity concerned officially being notified and legally named a suspect? Is the privacy violation proportional to the contribution made to investigative and prosecutorial outcomes? What institutional control mechanisms and safeguards are in place and what external control is there on the FIU's activities? These are important questions that should be at the centre of political and policy-related debates.

Notes

1. With some minor revisions, this paper was previously published in Dutch as Lagerwaard, P. (2022). Financiële surveillance en de rol van de FIU (FIU) in Nederland. *Beleid en Maatschappij* (49)2, 128-153. It was translated from Dutch to English by Liz van Gerrevink-Genee.
2. In Dutch, the "*Wet ter voorkoming van witwassen en financieren van terrorisme", Wwft*.

3. This course – undertaken in 2017 – was offered by the "Basel Institute on Governance", https://baselgovernance.org/elearning-courses/operational-analysis-english, consulted on 28 April 2021.
4. For annual reports, see www.fiu-nederland.nl/nl/over-fiu/jaaroverzichten, consulted on 14 June 2021. This paper often refers to the 2020 report for the data on 2019; and the 2021 report for the data on 2020 because these contain the most up-to-date information at the time of writing.
5. Reporting groups such as banks are expected to implement a "Know Your Customer" policy. In doing so, they are expected to identify, verify and in the case of entities such as companies or foundations, to establish the "Ultimate Beneficial Owners".
6. See for high risk countries www.fatf-gafi.org/countries/#high-risk, consulted on 8 June 2021.
7. See for the online reporting portal: https://meldportaal.fiu-nederland.nl/Home, consulted on 8 June 2021.
8. Cited from a Parliamentary Paper: "This *VROS* index not only includes investigations relating to criminal intelligence unit subjects, but also all investigations that last longer than a week and are aimed at crimes for which provisional custody is permitted" (Dutch House of Representatives Tweede Kamer, 1998).
9. This database of unusual transactions is anonymously compared in FIU.net, and only after further consultation with a foreign FIU and the transaction is officially declared as suspicious, can the foreign FIU use this information.
10. In particular, Sections 12–14, respectively, set out the institutional embedding, core tasks and responsibilities and juridical framework of the FIU.
11. The RIECs use these suspicious transactions, for example to organize "Confiscations" from criminals (RIEC-LIEC, 2020, p. 22).
12. See case law on terrorist financing here: https://uitspraken.rechtspraak.nl/#zoekverfijn/zt[0][zt]=financiering+van+terrorisme&zt[0][fi]=AlleVelden&zt[0][ft]=Alle+velden&so=Relevance&ps[]=ps1, consulted on 8 June 2021.

References

AFM, (Autoriteit Financiële Markten) (2020), "Leidraad wwft en sanctiewet: Toelichting op de wet ter voorkoming van witwassen en financieren van terrorisme en de sanctiewet 1977".

AG Connect (2008), "Politie is zeer tevreden over BlueView", *AG connect*, available at: www.agconnect.nl/artikel/politie-is-zeer-tevreden-over-blueview (accessed 17 May 2021).

Akse, T. (2019), "Na de poortwachters: 25 jaar meldingen ongebruikelijke transacties", *FIU-Nederland*.

Amicelle, A. (2011), "Towards a 'new' political anatomy of financial surveillance", *Security Dialogue*, Vol. 42 No. 2, pp. 161-178.

Amicelle, A. (2017a), "Policing through misunderstanding: insights from the configuration of financial policing", *Crime, Law and Social Change*, Vol. 69 No. 2, pp. 207-226.

Amicelle, A. (2017b), "When finance met security: back to the war on drugs and the problem of dirty money", *Finance and Society*, Vol. 3 No. 2, pp. 106-123.

Amicelle, A. (2020), "Right of entry: the struggle over recognition in the world of intelligence", *Political Anthropological Research on International Social Sciences (PARISS)*, Vol. 1 No. 2, pp. 243-272.

Amicelle, A. and Chaudieu, K. (2018), "In search of transnational financial intelligence: questioning cooperation between financial intelligence units", in King, C., Walker, C. and Gurule, J. (Eds), *The Palgrave Handbook of Criminal and Terrorism Financing Law*, Palgrave Macmillan, Cham.

Amicelle, A. and Favarel-Garrigues, G. (2012), "Financial surveillance: who cares?", *Journal of Cultural Economy*, Vol. 5 No. 1, pp. 105-124.

Amoore, L. and de Goede, M. (2008), *Risk and the War on Terror*, Routledge, London.

Anwar, T. (2020), "Unfolding the past, proving the present: social media evidence in terrorism finance court cases", *International Political Sociology*, Vol. 14 No. 4, pp. 382-398.

Armstrong, G. and Norris, C. (1999), *The Maximum Surveillance Society: The Rise of CCTV*, Berg Publishers, New York, NY.

Atia, M. (2007), "In whose interest? Financial surveillance and the circuits of exception in the war on terror", *Environment and Planning D: Society and Space*, Vol. 25 No. 3, pp. 447-475.

Audit Magazine (2019), "IIA quality assessment review: veel ervaring veel toegevoegde waarde", *Instituut van Internal Auditors Nederland (IIA Nederland) en de Stichting Verenigde Operational Auditors (SVRO)*.

Basel Institute on Governance (2017), "E-learning course operational analysis", available at: https://baselgovernance.org/elearning-courses/operational-analysis-english

Bauman, Z. and Lyon, D. (2013), *Liquid Surveillance: A Conversation*, Polity Press, Cambridge.

Belastingdienst (2022), "Ongebruikelijke transactie melden voor de wwft", available at: www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/belastingdienst/zakelijk/aangifte_betalen_en_toezicht/wwft-voorkomen-van-witwassen-en-terrorismefinanciering/verplichtingen/ongebruikelijke-transactie-melden,consultedon8June2021

Belcher, O. and Martin, L. (2019), "Site visits, selective disclosure, and freedom of information in qualitative security research", in de Goede, M., Bosma, E. and Pallister-Wilkins, P. (Eds), *Secrecy and Methods in Security Research: A Guide to Qualitative Fieldwork*, pp. 33-47, Routledge, London.

Bellanova, R. (2014), "Data protection, with love", *International Political Sociology*, Vol. 8 No. 1, pp. 112-115.

Bellanova, R. and Duez, D. (2012), "A different view on the 'making' of european security: the EU passenger name record system as a socio-technical assemblage", *European Foreign Affairs Review*, Vol. 17, pp. 109-124.

Bellanova, R. and Sætnan, A.R. (2019), "How to discomfort a worldview?", in Singh, J.P., Carr, M. and Marlin-Bennett, R. (Eds), *Social Sciences, Surveillance Technologies, and Defamiliarization*, Routledge, New York, NY, pp. 29-40.

Birchall, C. (2016), "Six answers to the question 'what is secrecy studies?'", *Secrecy and Society*, Vol. 1 No. 1, p. 2.

Bosma, E. (2019), "Multi-sited ethnography of digital security technologies", in de Goede, M., Bosma, E. and Pallister-Wilkins, P. (Eds), *Secrecy and Methods in Security Research: A Guide to Qualitative Fieldwork*, Routledge, London.

Bosma, E., de Goede, M. and Pallister-Wilkins, P. (2019), "Introduction: navigating secrecy in security research", in de Goede, M., Bosma, E. and Pallister-Wilkins, P. (Eds), *Secrecy and Methods in Security Research: A Guide to Qualitative Fieldwork*, Routledge, London, pp. 1-27.

Boy, N., Morris, J. and Santos, M. (2017), "Introduction: taking stock of security and finance", *Finance and Society*, Vol. 3 No. 2, pp. 102-105.

Dandeker, C. (2007), "Surveillance: basic concepts and dimensions", in Hier, S.P. and Greenberg, J. (Eds), *The Surveillance Studies Reader*, Vol. Hoofdstuk 3, Open University press, Berkshire, pp. 39-51.

de Boer, M. (2021), "Beleggers reageren opgelucht nu witwasboete ABN amro", *Het Financieele Dagblad*, available at: https://fd.nl/beurs/1380823/beleggers-reageren-opgelucht-na-witwasboete-abn-amro-qjf1caxuwzt3 (accessed 10 June 2021).

de Goede, M. (2010), "Financial security", in Burgess, J.P. (Ed.), *The Routledge Handbook of New Security Studies*, Chapter 11, Routledge, New York, NY, pp. 100-109.

de Goede, M. (2017a), "Banks in the frontline: assembling space/time in financial warfare", in Christophers, B., Leyshon, A. and Mann, G. (Eds), *Money and Finance After the Crisis*, John Wiley and Sons, pp. 117-144.

de Goede, M. (2017b), "Chains of securitization", *Finance and Society*, Vol. 3 No. 2, pp. 197-207.

de Goede, M. (2018), "The chain of security", *Review of International Studies*, Vol. 44 No. 1, pp. 24-42.

de Goede, M., Bosma, E. and Pallister-Wilkins, P. (2019), *Secrecy and Methods in Security Research: A Guide to Qualitative Fieldwork*, Routledge, London.

Dehouck, M. and de Goede, M. (2021), *Public-Private Financial Information-Sharing Partnerships in the Fight Against Terrorism Financing*, University of Amsterdam.

Dijstelbloem, H. and Pelizza, A. (2019), "The state is the secret: for a relational approach to the study of border and mobility control in Europe", in de Goede, M., Bosma, E. and Pallister-Wilkins, P. (Eds), *Secrecy and Methods in Security Research: A Guide to Qualitative Fieldwork*, Routledge, London, pp. 48-62.

DNB, (De Nederlandse Bank) (2020), "Leidraad wwft en Sw versie december 2020".

Egmont Group (2013), "Egmont group of financial intelligence units principles for information exchange between financial intelligence units", Egmont Group of Financial Intelligence Units.

Egmont Group (2017), "Egmont group of financial intelligence units operational guidance for FIU activities and the exchange of information", Egmont Group of Financial Intelligence Units.

European Commission (2016), "Gedelegeerde verordening (EU) 2016/1675 van de commissie", available at: https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:02016R1675-20181022&from=EN (accessed 6 May 2021).

European Commission (2017), "Commission staff working document: on improving cooperation between EU financial intelligence units".

Ferrari, V. (2020), "Crosshatching privacy: financial intermediaries' data practices between law enforcement and data economy", *European Data Protection Law Review*, Vol. 6 No. 4, pp. 522-535.

FIU-Nederland (2019), "FIU-Nederland jaaroverzicht 2018", available at: www.fiu-nederland.nl/sites/www.fiu-nederland.nl/files/documenten/fiu-nederland_jaaroverzicht_2018_nl_web.pdf

FIU-Nederland (2020), "FIU-Nederland jaaroverzicht 2019", available at: www.fiu-nederland.nl/sites/www.fiu-nederland.nl/files/documenten/jaaroverzicht_2019_-_fiu_nederland.pdf

FIU-Nederland (2021), "FIU-Nederland jaaroverzicht 2020", available at: www.fiu-nederland.nl/sites/www.fiu-nederland.nl/files/documenten/fiu_jaaroverzicht_2020nl.pdf

FIU-Nederland (2022a), "Handleiding GoAML", available at: https://meldportaal.fiu-nederland.nl/public_documents/Handleiding%20goAML%20Nederlands%20release%204%200%20(nieuw).pdf (accessed 5 August 2022).

FIU-Nederland (2022b), "Banken", available at: www.fiu-nederland.nl/nl/meldergroep/8 (accessed 8 June 2021).

FIU-Nederland (2022c), "Ben ik meldplichtig?", available at: www.fiu-nederland.nl/nl/melden/ben-ik-meldplichtig (accessed 5 May 2021).

FIU-Nederland (2022d), "Casuïstiek", available at: www.fiu-nederland.nl/nl/wetgeving/casuistiek (accessed 18 May 2021).

FIU-Nederland (2022e), "Moet ik rekening houden met de algemene verordening gegevensbescherming (AVG) bij het nakomen van de verplichtingen op grond van de wet ter voorkoming van witwassen en financieren van terrorisme (wwft)?", available at: www.fiu-nederland.nl/nl/faq#n1222 (accessed 4 January 2022).

FIU-Nederland (2022f), "Organisatie", available at: www.fiu-nederland.nl/nl/over-fiu/organisatie (accessed 8 June 2021).

Foucault, M. (1977), *Discipline and Punish: The Birth of the Prison*, Vintage Books, New York, NY.

Gilbert, E. (2015), "Money as a 'weapons system' and the entrepreneurial way of war", *Critical Military Studies*, Vol. 1 No. 3, pp. 202-219.

Haggerty, K.D. and Ericson, R.V. (2000), "The surveillant assemblage", *The British Journal of Sociology*, Vol. 51 No. 4, pp. 605-622.

Hendrikse, R., Bassens, D. and van Meeteren, M. (2018), "The appleization of finance: charting incumbent finance's embrace of FinTech", *Finance and Society*, Vol. 4 No. 2, pp. 159-180.

Jones, G.M. (2014), "Secrecy", *Annual Review of Anthropology*, Vol. 43 No. 1, pp. 53-69.

Kamphuis, B. (2021), "Een miljoen 'ongebruikelijke' transacties, maar weinig aanhoudingen", *NOS*, available at: https://nos.nl/nieuwsuur/artikel/2403990-een-miljoen-ongebruikelijke-transacties-maar-weinig-aanhoudingen (accessed 4 December 2021).

KLPD, (Korps landelijke politiediensten) (2008), "Witwassen: verslag van een onderzoek voor het nationaal dreigingsbeeld 2008", avaialble at: https://docplayer.nl/1602433-Witwassen-verslag-van-een-onderzoek-voor-het-nationaal-dreigingsbeeld-2008-klpd-dienst-ipol.html

Lagerwaard, P. (2018), "Following suspicious transactions in Europe: comparing the operations of European financial intelligence units (FIUs)", FOLLOW Research Report, Amsterdam Institute for Social Science Research (AISSR), Amsterdam.

Lagerwaard, P. (2020), "Flattening the international: producing financial intelligence through a platform", *Critical Studies on Security*, Vol. 8 No. 2, pp. 160-174.

Langley, P. (2017), "Finance/security/life", *Finance and Society*, Vol. 3 No. 2, pp. 173-179, doi: 10.2218/finsoc.v3i2.2576.

Latour, B. (1999), *Pandora's Hope: Essays on the Reality of Science Studies*, Harvard University Press, Cambridge/London.

Lupton, D. (2012), "M-health and health promotion: the digital cyborg and surveillance society", *Social Theory and Health*, Vol. 10 No. 3, pp. 229-244.

Lyon, D., Haggerty, K.D. and Ball, K. (2012), "Introduction surveillance studies", in Ball, K., Haggerty, K.D. and Lyon, D. (Eds), *Routledge Handbook of Surveillance Studies*, Routledge, New York, NY, pp. 1-12.

Ministry of Justice, Netherlands (2008), "Wet ter voorkoming van witwassen en financieren van terrorisme (wwft)".

Mitsilegas, V. and Vavoula, N. (2016), "The evolving EU anti-money laundering regime: challenges for fundamental rights and the rule of law", *Maastricht Journal of European and Comparative Law*, Vol. 23 No. 2, pp. 261-293.

Mouzakiti, F. (2020), "Cooperation between financial intelligence units in the European Union: stuck in the middle between the general data protection regulation and the police data protection directive", *New Journal of European Criminal Law*, Vol. 11 No. 3, pp. 351-374.

Nadrous, F. (2020), "Tienduizenden witwasmeldingen, amper strafzaken. 'soms lijkt het of het hele meldsysteem voor niets is'", *Trouw*, available at: www.trouw.nl/economie/tienduizenden-witwasmeldingen-amper-strafzaken-soms-lijkt-het-of-het-hele-meldsysteem-voor-niets-is~b03c7f64/ (accessed 8 June 2021).

Nu.nl (2007), "Politie kan criminelen 'googelen'", *Nu.nl*, available at: www.nu.nl/internet/1106457/politie-kan-criminelen-googelen.html (accessed 17 May 2021).

Orwell, G. (1949), *Nineteen Eighty-Four*, Penguin, New York, NY.

RIEC-LIEC (2020), "RIEC-LIEC jaarverslag 2019", available at: www.riec.nl/documenten/jaarverslagen/2019/06/23/riec-liec-jaarverslag-2019

Riemslag Baas, A.M. (2021), "De bijdrage van banken aan het voorkomen en bestrijden van witwassen en terrorismefinanciering", *Tijdschrift Financieel Recht in de Praktijk*, Vol. 1, pp. 45-51.

Timan, T. and Grommé, F. (2020), "Wat is rechtvaardige AI?: Een kader voor het ontwikkelen en toepassen van algoritmes voor automatische besluitvorming", *Beleid en Maatschappij*, Vol. 47 No. 4, pp. 425-438.

Tweede Kamer (1998), "Uitwisseling van recherche-informatie tussen CRI en politieregio's", Tweede Kamer der Staten-Generaal, available at: https://zoek.officielebekendmakingen.nl/kst-26215-4.pdf

Van Dijck, J. (2014), "Datafication, dataism and dataveillance: big data between scientific paradigm and ideology", *Surveillance and Society*, Vol. 12 No. 2, pp. 197-208.

VIRBI (2013), "Besluit voorschrift informatiebeveiliging rijksdienst bijzondere informatie 2013", available at: https://wetten.overheid.nl/BWBR0033507/2013-06-01 (accessed 8 June 2021).

Vlcek, W. (2007), "Surveillance to combat terrorist financing in Europe: whose liberty, whose security?", *European Security*, Vol. 16 No. 1, pp. 99-119.

Vlcek, W. (2009), "Hitting the right target: EU and security council pursuit of terrorist financing", *Critical Studies on Terrorism*, Vol. 2 No. 2, pp. 275-291.

Weller, T. (2012), "The information state: an historical perspective on surveillance", in Ball, K., Haggerty, K.D. and Lyon, D. (Eds), *Routledge Handbook of Surveillance Studies*, Routledge, New York, NY, pp. 57-63.

Westermeier, C. (2019), "Political security and finance – a post-crisis and post-disciplinary perspective", *Zeitschrift Für Politikwissenschaft*, Vol. 29 No. 1, pp. 105-122.

Westermeier, C. (2020), "Money is data – the platformization of financial transactions", *Information, Communication and Society*, Vol. 23 No. 14, pp. 2047-2063.

Zuboff, S. (2019), *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Profile Books, London.

Corresponding author
Pieter Lagerwaard can be contacted at: pieterlagerwaard@gmail.com