3. National threats of money laundering and terrorist financing

3.1. Nature and extent of money laundering in Estonia

The definition of money laundering in Estonian law derives from § 4 of the Money Laundering and Terrorist Financing Prevention Act pursuant to which "money laundering" means the conversion or transfer of property derived from criminal activity or property obtained instead of such property for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's actions; the acquisition, possession or use of property derived from criminal activity or property obtained instead of such property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation therein; the concealment of the true nature, origin, location, manner of disposal, relocation or right of ownership of property acquired as a result of a criminal activity or property acquired instead of such property or the concealment of other rights related to such property. Money laundering also means participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the activities referred to above.

In compiling the Estonian 2015 National Money Laundering Risk Assessment[1], proceedings involving criminal offences, including money laundering offences, in 2010-2012 were analysed. In the National Risk Assessment it was concluded, among other things, that the number of cases of money laundering and predicate offences is relatively limited. Most predicate offences involved computer fraud or fraud (and embezzlement) committed abroad. Other criminal offences were predicate offences only in isolated cases (unlawful handling of large quantities of narcotic drugs or psychotropic substances; membership in a criminal organisation; use of a falsified document; economic activities without an activity license, and prohibited economic activities; tax fraud).

Similarly to the 2015 National Risk Assessment, the described situation remains relevant for this Risk Assessment. At the same time, we must note that considering a number of possible money laundering cases that have occurred within the time period of 2017-2019, and ongoing proceedings, potential risks have increased as compared to the time of the previous Risk Assessment.

This National Risk Assessment is based on registered and investigated crimes as well as court decisions that took effect within the time period of 2017-2019.

Money laundering, i.e. criminal offences under § 394 of the Penal Code, were registered as follows:

- 2017 – 41
- 2018 – 101
- 2019 – 190

The number of court decisions that took effect in proceedings commenced on the basis of § 394 of the Penal Code was as follows:

- 2017 – 14
- 2018 – 7
- 2019 – 12

Natural persons were convicted of committing a criminal offence provided for in § 394 of the Penal Code as follows:

- 2017 – 39

[1] Estonia's 2015 National Money Laundering and Terrorist Financing Risk Assessment is available at https://www.rahandusministeerium.ee/system/files_force/document_files/ohuhinnangu_tulemuste_kokkuvote_rm_avalik.docx?download=1

- 2018 – 16
- 2019 – 22

Legal persons were convicted of committing a criminal offence provided for in § 394 of the Penal Code as follows:

- 2017 – 3
- 2018 – 1
- 2019 – 1

Although § 394[1] of the Penal Code prescribes liability for money laundering agreement[2], no criminal offences under § 394[1] of the Penal Code were registered during this period and, consequently, there are no court decisions that have taken effect.

At the same time, in the light of these statistics, it is important to emphasise that while recorded crimes may concern individual episodes, court decisions may reflect on completed criminal proceedings. As episodes concerning one person or event are combined into one criminal case, this also explains the numerical difference between these categories.

It is also important to note that there is no direct correlation between registered crimes and effective court decisions. Thus, proceedings in many criminal cases and judgments that took effect within the 2017-2019 time period had been commenced significantly earlier. In addition, a court decision might not have taken effect by now in all criminal offences registered within the relevant period. Due to the complexity of money laundering proceedings, including the need to use international cooperation measures, pre-court and court proceedings can take years.

In the case of money laundering, pursuant to its definition, it is important for the property to have been acquired as a result of criminal activity, i.e. a criminal offence (a predicate offence) has been committed. The commission of a predicate offence and criminal origin of property is a precondition for the activities related to the relevant property to be considered money laundering. A predicate offence may have been committed by another person and it may have been committed abroad.

In most cases, the predicate offence to a money laundering crime was computer fraud or fraud and, generally speaking, these crimes were committed outside of Estonia and by persons not identified during criminal proceedings. In such cases, the persons were convicted only of committing the criminal offence of money laundering.

The following could be pointed out in the case of the 77 natural persons convicted from 2017 to 2019. The commission of a predicate offence was established in the case of 28 persons (self-laundering); in the case of 49 persons, the predicate offence was committed by a third party (third party laundering). While in the case of self-laundering cases, predicate offences were mostly computer crimes, fraud, and membership in a criminal organisation, in the case of third party laundering, the predicate offences were computer crimes, fraud, and tax fraud.

In individual cases, in the course of proceedings, the perpetration of a predicate offence by the person was also established in addition to the money laundering crime. The courts also confiscated the assets or property acquired by the criminal offence. In cases where the assets or property acquired by the criminal offence had, for example, been transferred or consumed, substitution of confiscation was

[2] **§ 394[1] of the Penal Code. Money laundering agreement**
(1) Conclusion of an agreement for the purpose of execution of money laundering,
is punishable by a pecuniary punishment or up to two years' imprisonment.
(2) The same act, if committed by a legal person,
is punishable by a pecuniary punishment.

applied[3] and payment of an amount corresponding to the value of the property to be confiscated was ordered.

Assets were confiscated in proceedings related to money laundering offences in the amount of EUR 700,537.64 in 2017, EUR 509,075.3 in 2018 and EUR 993,070.97 in 2019. The assets confiscated were in the form of cash, money in bank accounts, movable and immovable property.

Most cases of money laundering offences were related to predicate offences committed outside of Estonia, and, generally speaking, the role of the persons located in Estonia was to receive money transferred from abroad and to transfer it to other persons.

The following court decisions that took effect in 2018 and 2019 are examples of the above possible cases.

By Judgment No. 1-18-8950, seven natural persons were convicted of money laundering, three of whom were also convicted of formation and being a member of a criminal organisation (§ 255 and § 256 of the Penal Code, respectively). In this case, the predicate offence entailed tax fraud and accounting crimes committed in the Republic of Finland and the concealment of the origin and conversion in Estonia of the proceeds of the above crimes in the amount of more than 4.2 million euros. In the criminal case, property totalling 67,358 euros was seized and property totalling 81,157 euros was confiscated.

By Judgment No. 1-19-5475, two natural persons were convicted of committing money laundering and aiding and abetting fraud (§ 209 of the Penal Code). The predicate offence consisted of forwarding falsified authorisations to legal persons by e-mail and requesting bank transfers into the bank account of a previously established Estonian legal person. Money was received into the bank account of the legal person established in Estonia in the total amount of nearly 800,000 euros. The money received into the bank account of the legal person established Estonia was transferred to other bank accounts, including those located abroad, and partly withdrawn in cash in Estonia. In most part, the transfer of the relevant money was blocked by the Financial Intelligence Unit. In this criminal case, 635,161.32 euros were seized and later confiscated.

It is also important to note that criminal proceedings are still pending concerning alleged money laundering in two cases of importance for Estonia (Danske Bank A/S Estonia Branch and Swedbank AS). Both criminal proceedings are currently of the highest priority for national law enforcement authorities in the field of money laundering.

3.1.1. Nature of predicate offences to money laundering and extent of money laundering in Estonia

I. Background and statistics of money laundering and predicate offences

This National Risk Assessment is based on data for the 2017-2019 time period. There are relatively few registered money laundering offences and related court decisions as compared to other criminal offences and court decisions. On the average, 9-12 court judgments a year took effect during this time period.

Based on cases that have been proven in court, it can be stated that predicate offences to money laundering are mostly committed outside of Estonia and the perpetrators of predicate offences are often not identified during the criminal proceedings. The role of persons convicted in Estonia has

[3] **§ 84 of the Penal Code. Substitution of confiscation**
If the assets acquired by an offence in the meaning of § 83^1 of this Code or assets acquired by a criminal offence in the meaning of § 83^2 of this Code, the instrument by which a criminal offence was committed or the direct object of a criminal offence have been transferred, consumed or the confiscation thereof is impossible or unreasonable for another reason, the court may order payment of an amount which corresponds to the value of the assets subject to confiscation.

mostly consisted in enabling the transfer of funds to their personal bank account or to the bank account of a legal person set up to commit money laundering which are then either transferred to other bank accounts or withdrawn in cash and passed on. In individual cases, it has been established that the perpetrator of money laundering has also committed the predicate offence.

In the case of money laundering, it is important to establish the facts of concealment or conversion of property acquired as a result of criminal activity or property acquired instead of such property. Consequently, predicate offences include the types of criminal offences and cases that generate proceeds acquired by criminal activity, the origin of which is later concealed.

In the time period of 2017-2019, 32 convictions took effect regarding the perpetration of money laundering, i.e. an act provided for in § 394 of the Penal Code. A total of 77 natural persons were convicted. 5 legal persons were convicted.

Predicate offences mostly included fraud and computer fraud, and in most cases have been committed outside of Estonia.

- Four judgments concerned tax offences, three of which were committed in the Republic of Finland.
- In the case of 13 judgments, the predicate offence was computer fraud.
- In the case of 9 judgments, the predicate offence was fraud.

In most cases, predicate offences are committed outside of Estonia and by persons who could not be identified during the investigation. In individual cases, the commission of a predicate offence outside of Estonia by persons convicted of money laundering was established, especially in the case of fraud and computer fraud.

In most cases, persons convicted of money laundering in Estonia have not committed predicate offences themselves, in some cases participation in the commission of a predicate offence has been established during the investigation, and persons have also been convicted of aiding and abetting a predicate offence. However, the perpetrators of the crime have not been identified in such a case.

Assets that were the object of money laundering identified by a court judgment and the amounts have varied during the time period. There have been cases where the object of money laundering is an asset worth a few thousand euros, while there have also been cases where the object of money laundering has been funds in the total value of 1.1 million euros, 2 million euros, and 4.2 million euros, respectively. In seven cases the value of money laundered was between 5,000 and 50,000 euros, and in thirteen cases between 100,000 and 500,000 euros.

Also worth mentioning is clause 25 of the Supreme Court's judgment No. 3-1-1-34-05 pursuant to which the commission of money laundering must be the main purpose of the person and the act van not be considered money laundering if the property acquired as a result of criminal activity is consumed.
Consequently, if money laundering was not the person's goal and the property acquired as a result of the criminal activity is simply consumed, then pursuant to Estonian court practice, it is not money laundering (self-laundering).

The relevant Supreme Court's decision has been further specified by Tartu Circuit Court in its decision No. 1-15-6497, where, among other things, the following was noted:

"In order to speak of the use of assets acquired by criminal activity as money laundering, the act to be subsumed must also have real potential to undermine the normal functioning of the economy. The functioning of the financial or economic system as a whole is not primarily impaired by the handling of assets obtained by criminal activity for personal consumption and not for the purpose of exploiting the financial or economic system where assets are first cleaned of their original criminal background

and only thereafter used for any lawful purpose. In other words, if the way in which assets acquired by criminal activity are handled does not harm the performance of financial or economic system of the state, it cannot be considered money laundering even if the use of the assets involves the concealment of their true origin.
Consequently, money laundering is primarily concerned with the protection of the state's financial and economic system from manipulation involving assets acquired by criminal activity, and not with any use of assets acquired by criminal activity during which the true origin of the assets remains concealed.
In order for the necessary elements of the offence of money laundering to be present, the concealment of the illegal origin of the assets and their beneficial owner must play a central role in the legal acts undertaken with the assets acquired by criminal activity. There is no money laundering if the concealment of the illegal origin of the assets and the beneficial owner is merely an ancillary purpose or a consequence in the transactions undertaken with such assets.
Consequently, for the necessary elements of the offence of money laundering to be present, especially where the perpetrator of money laundering is also the perpetrator of a predicate offence, the relevant concealment activities must have a certain quality which would, on the one hand, pose an independent threat to the orderly functioning of the financial and economic system and, on the other hand, distinguish the money laundering offence from the perpetrator's normal activities in concealing their crime and the assets acquired thereby."

For the above reason, self-laundering can be spoken of only in cases where the perpetrator of the predicate offence has also begun to perform various acts as pertaining to the assets acquired by the criminal offence in order to conceal the origin thereof.

This in turn allows the following **conclusions** to be drawn:

- Persons located and prosecuted in Estonia have mostly been involved only in the perpetration of money laundering, in individual cases they have been identified and convicted of committing or aiding and abetting a predicate offence.
- In order to organise money laundering, both natural and legal persons are exploited in Estonia, whose role have been to use their bank accounts for receiving and transferring money for a fee. The amounts received are largely transferred, withdrawn in cash and passed on, and individuals have retained a certain fee for this.
- The perpetrators of predicate offences are looking for persons in Estonia to exploit in organising money laundering. Often, legal persons are set up and bank accounts are opened for them for money laundering purposes.
- Money received on bank accounts of natural and legal persons located in Estonia mostly comes from foreign countries and is often transferred on to other bank accounts located abroad.

Where criminal proceedings are commenced, the property of both natural and legal persons is seized for the purpose of securing a civil action or confiscation. Regardless of whether the person has committed money laundering or if they have also been involved in the perpetration of a predicate offence, it is possible to seize property acquired from the crime. If the person has acted as an intermediary and has only participated in organising money laundering, the seized property is often limited to the assets the person received in return for organising money laundering.

The FIU has often intervened and set restrictions on the use of bank accounts in relation to the identification of suspicious or unusual transactions. This has in most cases ensured that the transfer of funds to bank accounts abroad has been prevented and it has been possible to seize the money on the relevant bank accounts to secure either a civil action or confiscation.
In practice, extended confiscation and confiscation of third party property have been applied to money laundering offences, and also substitution of confiscation has been applied when assets acquired as a result of the crime have been transferred or spent.

II. Predicate offences to money laundering

Focussing on the inherent functioning of money laundering, threats at the national level emerge in the following places:

Emergence of assets obtained by criminal activity

In Estonia, all criminal offences listed in the Penal Code constitute predicate offences to money laundering. At the same time, there is a presumption in the definition of money laundering that money must emerge that needs to be laundered, i.e. a money laundering offence cannot be committed without the emergence of financial gain.

The Yearbooks of the Financial Intelligence Unit list money laundering schemes that stood out in different years, about which information has been received from obliged entities and on which analyses has also been disseminated to law enforcement authorities. A criminal offence committed in another country, property acquired as a result of which is laundered in our country, can also be considered a predicate offence to money laundering. Here, it is important to monitor which geographical areas are most important for Estonia in order to be ready to deal with this threat.

The NRA covers the time period of 2017-2019, and the most important schemes in those years were the following:

1) Cyber fraud. The volume and worldwide nature of this type of crime is increasing year by year, and the FIU has had to deal with these crimes in all the years covered by the NRA. In 2019, cases of investment fraud were added, which by their nature constituted, rather, ordinary fraud committed in the cyber world and did not actually involve investment services. Companies with service providers that exchange virtual currency for money and companies that hold activity licenses for wallet services, all registered in Estonia, that do not have the right to provide investment services within the framework of the relevant license were also taken advantage of.
2) Fraud related to small loan companies. Bank accounts are opened on behalf of third parties and thereafter loans are taken from various small loan companies without any intention to pay them back. Relevant in both 2017 and 2018.
3) Perpetration of tax fraud. In the case of tax fraud, it is difficult to identify the damage caused in cases where false information is submitted in tax returns for the purpose of reducing the VAT liability. It is easier to understand the emergence of proceeds obtained by criminal activity if claims for refund of the amounts of VAT paid are submitted which lack actual substance of economic transactions. In such a case, the amount embezzled from the tax authority constitutes proceeds of criminal activity, the different phases of money laundering of which are clearer to monitor. In most cases, money is quickly transferred from an Estonian bank account to foreign settlement or payment accounts.
4) Withdrawal of money with falsified bank cards. This activity is usually preceded by withdrawal of fraudulently obtained assets or of money transferred to falsified bank cards on the basis of stolen bank card data.
5) Cash flows of suspicious origin in legal business. It is not clear here from what crime the cash flows were obtained, but their movement indicates the perpetration of money laundering. In most cases, the layering phase can be observed.
6) Moving of property acquired as a result of a crime of corruption or embezzlement committed abroad (mostly in the former member states of the Soviet Union) to the Estonian financial system in order to direct it back to criminals or invest it in real estate and businesses in Estonia. There is also a time lag between the predicate offence and identification of the relevant money, on account of which it is difficult to seize property. It is complicated to obtain information on a predicate offence because foreign cooperation takes time or the relevant countries are not cooperative.
7) Bankruptcy offences. Pursuant to § 45 of the Bankruptcy Act, it is possible to escape seizure applied with regard to a debtor's assets before the declaration of bankruptcy terminates. This was used when criminal proceedings had been instituted against a legal person, in the framework of which property was seized, but criminal offenders still wanted to release the property acquired by their criminal activity.

8) Corruption offences and politically exposed persons.

Additional threat is posed by other predicate offences that generate proceeds, but information about them has not reached the FIU through reports from obliged entities. For example proceeds of large-scale drug crimes, proceeds acquired by organised crime, which should constitute a greater threat to the Estonian financial system and economy. The FIU usually receives information about these persons and activities through requests made in criminal proceedings.

Threats related to the concealment of the origin of assets obtained by criminal activity and layering of such assets as well as to the perpetration of possible new crimes:

1) Exploitation of companies
    a. Establishing companies in Estonia is easy, fast, and affordable. The threat here is the fact that, so as to hide one's tracks, it is possible to quickly set up several companies for one person, through which proceeds acquired by criminal activity can be moved. Also the use of figureheads to conceal the beneficial owner. A company may also be owned by a non-resident, although in such an event it must have a local address through which the state can contact it. The threat lies in taking advantage of this opportunity because when selling companies to non-residents, it is difficult to contact the beneficial owners, especially if the relevant operations do not take place in Estonia.
    b. Criminal offenders buy companies at a price that is not in conformity with the company's economic activity or business potential. If it is not possible to verify the origin of foreign capital, there is a high risk that money of unclear or criminal origin will flow into the Estonian financial system.
2) Exploitation of obliged entities
    a. The organisational set-up of obliged entities is not always appropriate for preventing money laundering and terrorist financing. The management must be interested and take available measures to ensure that both the relevant regulation and employees are prepared to contribute. Business interests and risk appetite cannot exceed the due diligence required to combat money laundering and terrorist financing.
    b. Due diligence measures are not implemented sufficiently. If companies that help manage funds (credit institutions, financing institutions, and other obliged entities) do not apply sufficient due diligence measures to identify their customers, it is possible that their services can be used to transfer funds obtained by criminal activity. With the development of financial technology, application of due diligence measures can be arranged through technical means. The threat there is that a person will be exploited forcibly or for financial gain to open a bank account for themselves, the beneficial owner of which is a third party. E-residency is definitely a threat here, as it is not always possible to efficiently identify the person or supervise their activities.
    c. Suspicious transaction tracking systems are not efficient and suspicious transactions are not recognised. Therefore, transactions are not sufficiently analysed and the FIU is not notified.
    d. Employees are not sufficiently trained or motivated to be able to identify suspicious transactions and, at the same time, not to be exploited by criminal offenders not to apply due diligence measures to certain transactions.
3) Money acquired by criminal activity is in the form of cash and various fictitious documents are prepared to explain its origin – (loan) agreements, invoices, etc.
4) Assets are moved through the services of various financial service providers – payment services, investment instruments, gambling service providers. Different service providers have different risk appetites and different levels of applying due diligence measures.
5) Financial services are used only to quickly move assets from the country that committed the predicate offence between the countries where the different phases of money laundering are perpetrated – i.e. transit transfers. The threat lies in not identifying criminal offenders, because they are linked to a country that the cash flow traversed only by a settlement account or a payment account. The companies used may be registered either in Estonia or abroad, but

their activities are not related to Estonia and, therefore, the perpetrators cannot be identified. Suspending the movement of assets is also problematic if the financial institution serving the payment has not set up its monitoring systems properly.

6) Assets are moved through virtual currencies. The activities of the providers of this service are regulated in Estonia. At the same time, the level of market entry is relatively low and there are too many virtual currency service providers for the small-sized market of Estonia (419 as of 31 December 2020). In addition, problematic is the fact that many companies with non-resident owners enter the service providers' market with the objective of obtaining an activity license issued by a supervisory authority by which they can demonstrate that their activities can be verified by a public authority and that their activities are legitimate. However, this matter is mere words as it is not possible to efficiently supervise the relevant persons' activities that are not located in the territory of the supervising state. However, it allows companies providing virtual currency services to operate as convenient and suitable for their customers, without taking into account the fact that they, as obliged entities, are subject to increased requirements in terms of preventing money laundering and terrorist financing. The product offered by the service – virtual currency – is by nature a rapidly evolving technology that changes owners digitally. Moving assets virtually is extremely fast and concealing one's tracks is also easy using various asset mixers. Although the movement of virtual assets generally leaves a public trace, the wallet owners' information is not public and it is also difficult to trace the route of assets that have gone through the mixers. In addition, it is easier to open virtual wallets or asset pools than a credit institution's account in different countries, causing an existing threat here. Especially where the service provider has not applied appropriate due diligence measures to exclude persons with suspicious or criminal backgrounds from its customer base and has not contributed to the establishment of efficient monitoring systems to make sure suspicious transactions are traceable.
7) Criminal offenders use trade-based money laundering to move ever new funds of criminal origin through various commodity-related schemes (such as overpricing and underpricing, one commodity moves multiple times based on different invoices, etc.).
8) Use of customs warehouses. Goods are not declared in a customs warehouse unless they enter the country. The operator of the customs warehouse does not have an overview of how the goods are resold and at what price or how they are paid for.
9) Cross-border movement of cash or goods to cover one's tracks and render identification of origin as time-consuming and complex as possible. It is also possible to avoid control by using ostensible or partial declarations.

<u>Property acquired by criminal activity</u> <u>has become part of legal economy which is hard to identify</u>
Criminal offenders have already been able to turn their assets acquired by criminal activity into a part of the legal economy:

a) by owning companies, the capital of which consists of assets acquired by criminal activity but the activities and earned profit of which are legal;
b) by sale and purchase of shares traded on the stock market;
c) by modifying the company's revenue base to consist in part of proceeds of criminal activity but the percentage of such proceeds is kept small, approximately 10-20% and is not noticeable in their economic activities' general turnover;
d) as real estate purchased for assets obtained by criminal activity is being used as housing or for earning rental income;
e) by use of luxury goods and services;
f) by acquisition of real estate, or share capital of companies with virtual currencies.

Once the funds acquired by criminal activity have passed the integration phase, i.e. used in legal economy and consumption, it becomes considerably more difficult to detect.

Based on the criminal statistics for the 2017-2019 time period, it can be concluded that the probability of money laundering in Estonia is higher in the case of computer crimes and fraud. These have also been the types of crime in the case of which the perpetrator of a predicate offence was often found to

have committed the money laundering offence as well. For other types of crime, the likelihood of related money laundering could be considered low, rather, and this is also supported by available data and criminal statistics. Court decisions that have taken effect have identified money laundering amounting to hundreds of thousands of euros, in individual cases to millions. At the same time, the number of such cases is relatively small.

It is frequently possible to detect larger amounts in cases where the predicate offences are either fraud or tax fraud.

While, in general, persons located in Estonia commit crimes on the territory of Estonia, it is important to point out in the case of computer fraud and fraud that perpetration of a predicate offence is often directed from outside of Estonia and the victims are also located abroad.

III. Threat level of money laundering crimes

The threat level arising from predicate offences to money laundering in Estonia is considered low. Not many criminal proceedings for suspected money laundering are commenced compared to other types of criminal proceedings. In 2017, 41 relevant criminal offences were registered; in 2018, 101 offences; and in 2019, 191 criminal offences. However, the total number of registered criminal offences during the same period was 26,929, 27,125, and 27,169, respectively.[4]

On the average, 9-12 convictions for committing a money laundering offence enter into force every year. The total number of criminal cases resolved in court proceedings in county courts is as follows: 2017 – 6,802; 2018 – 5,749; 2019 – 15,346.[5]

It is important to note once again that a single criminal case may involve several convicted persons as well as several different episodes of crime registered as separate criminal offences. There are no statistics available that take into account the number of episodes included in the relevant proceedings in court.

In addition, it is important to point out the time lag between the registered crimes and the taking effect of the judgment. Investigating money laundering offences can be time consuming, especially if multiple individuals or multiple episodes of crime are involved. If a predicate offence or a money laundering offence is connected to a foreign country, it may be necessary to take international cooperation measures and gather evidence abroad. Thus, it may be that no judgment has taken effect as of yet for a criminal offence registered during the relevant time period.

Criminal statistics and other data do not indicate a very strong connection between the crimes committed in Estonia and money laundering. In most cases, predicate offences have been committed in other countries and money laundering perpetrated in Estonia is related to crimes committed outside of Estonia. The role of persons convicted of money laundering in Estonia has mostly consisted in organising money laundering, enabling a bank account to receive bank transfers, and transferring the amounts received. As a result, it can be concluded that in Estonia money laundering services are mostly offered to the perpetrators of predicate offences.

To summarise the relevant analysis results, it can be stated that in most cases predicate offences consist in computer fraud and fraud perpetrated abroad, laundering of money that has moved here in the stratification or integration phase within the framework of perpetration of corruption and embezzlement committed in CIS countries, also tax crimes committed in European countries, and, to a lesser extent, drug money laundering.

[4] Source: www.kriminaalpoliitika.ee
[5] Source: www.kohus.ee

Seizure and subsequent confiscation of property are applied increasingly more. Within the framework of court judgments, more and more property is confiscated but the amounts are generally small compared to the amount of the (suspected) predicate offence as only relatively small amounts are confiscated in the case of computer fraud as compared to assets subjected to money laundering (often up to 5%-10% of the total amount) that figureheads have received for allowing their accounts to be used. In other isolated cases (for example, in cases where the FIU has imposed restrictions on the use of bank accounts), it has been possible to also seize and confiscate larger amounts.

3.1.2. Nature and extent of international cash flows in Estonia

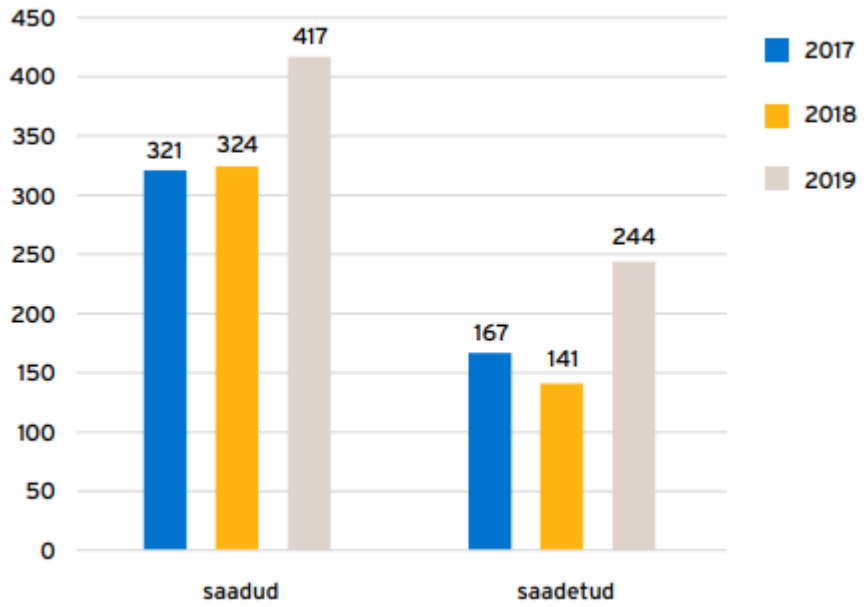
Cash flows to and from Estonia are mostly related to neighbouring countries and main trading partners. In preparing the National Risk Assessment, cash flows that took place during the 2017-2019 time period, both in and out of the country, have been analysed as pertaining to trade in goods, provision of services, investments, and remittances.

In terms of countries, immediate neighbours such as Finland, Latvia, Lithuania, the Russian Federation as well as Sweden, Norway, and Great Britain can be highlighted here.

Considering the general volumes of cash flows and comparing these to the amounts that have been proven in criminal proceedings related to money laundering, it is not possible to identify threats or risks related to money laundering on the basis of cash flows alone. Although most predicate offences are committed abroad, the countries from which money has been sent to Estonia and to which the money is in turn sent onwards from Estonia vary greatly. At the same time, it is necessary to take into account that cash flows concern trade in goods, services, and investments as well as remittances, and perpetration of money laundering offences cannot be presumed on the basis of cash flows. Therefore, cash flows cannot always be linked to international cooperation pertaining to money laundering prevention and criminal proceedings.

In terms of pre-trial proceedings for money laundering offences, Estonia also participates in international cooperation. During the 2017-2019 time period, 112 European Investigation Orders and 60 requests for mutual legal assistance were submitted by other countries to Estonia for execution; Estonia has submitted 51 European Investigation Orders and 39 requests for mutual legal assistance to other countries. Information exchange of the Financial Intelligence Unit with its foreign partners has been increasing every year. As FIUs generally share information on suspected money laundering transactions, in addition to inquiries in specific criminal proceedings, the cases analysed are often still in the phase of endeavours to prove suspected money laundering.

Figure 1. Number of foreign inquiries received and sent by the FIU in 2017-2019



Source: 2019 Yearbook of the Financial Intelligence Unit

As there is no obligation to declare cash when crossing the border within the European Union, statistics are only available for countries outside of the European Union. Among such countries, the Russian Federation and the United Arab Emirates (hereinafter UAE) can be noted in terms of cash incoming to country, the Russian Federation (hereinafter RF) in terms of outgoing cash.

Table 5. Cash flows incoming to Estonia from UAE and RF in 2017-2019

Country	2017	2018	2019		
	Declared cash, EUR	Declared cash, EUR	Declared cash, EUR	Number of declarations 2017-2019	Total declared cash, EUR 2017-2019
AE	8,116,988	5,736,950	14,597,603	150	28,451,541
RU	7,083,260	11,406,063	7,824,080	614	26,313,403

Table 6. Cash flows outgoing from Estonia towards China, Norway, and the RF in 2017-2019

Country	2017	2018	2019		
	Declared cash, EUR	Declared cash, EUR	Declared cash, EUR	Number of declarations 2017-2019	Total declared cash, EUR 2017-2019
CH	47,753,421	17,031,523	12,188,968	67	76,973,912
NO	15,420,452	13,108,171	7,907,972	141	36,436,595
RU	6,691,262	7,236,139	3,058,727	304	16,986,128

3.4. Nature and extent of cross-border money laundering in Estonia

In the case of geographical or cross-border threats, three groups of countries were analysed upon preparing the Risk Assessment: EU Member States, a number of non-EU countries, and a number of offshore countries. The selection was, among other things, based on assessment of potential cash flows as well as money laundering and terrorist financing risks.

Closer cooperation, spontaneous exchange of information, and the number of both incoming and outgoing cross-border requests for judicial assistance are the greatest among the Member States of the European Union. Cooperation and exchange of information is most substantial in the case of Latvia, Lithuania, Great Britain, Germany, and Finland.

With regard to countries outside of the European Union, there is closer cooperation with the Russian Federation, the United States of America, Belarus, and Ukraine.

For offshore countries, analysis was based on Gibraltar, Guernsey, the Isle of Man, Jersey, and the Cayman Islands, where information exchange has taken place only in a few cases.

Based on the criminal statistics for and court decisions that have taken effect during the 2017-2019 time period, it is not possible to assess threats or risks related to money laundering as pertaining to countries. Predicate offences such as fraud or computer fraud have been perpetrated in different foreign countries, and Estonia has been used as a transit country for the concealment of money laundering and for the concealment or conversion of the origin of assets acquired by criminal activity. As predicate offences have been committed in different countries, the origin of money sent to Estonia in relation to money laundering is also varied; money has also been transferred from Estonia to bank accounts in various other countries.

In terms of geographical or cross-border threats, no specific country or region can be highlighted as constituting a higher risk of money laundering. Estonia's neighbouring countries can be noted as an exception, with whom there is more cooperation and information exchange.

Since 2008, the FIU also issues activity licenses to alternative payment instrument service providers that were replaced by two groups of virtual currency service providers by relevant legislative amendment in 2017: the providers of the service of exchanging virtual currency for money and virtual currency wallet service providers; for the purposes of the current legislation, both of the above are included under the common designation of "virtual currency service providers". As from 2017, the popularity of the virtual currency service exploded, and as Estonia was one of the first to issue activity licenses to operate in this field, thousands of individuals around the world saw this as an opportunity. In 2017-2019 licenses were issued in Estonia to more than 1,300 businesses. Among them were also persons weaving criminal schemes, and companies with an Estonian activity license were exploited to commit various crimes abroad. The threat here was that the license was not valid for companies operating abroad but seemed to serve as a way to improve one's legitimacy. Company service providers saw a new market segment and quickly established companies providing virtual currency services with a FIU license which were also sold in large numbers to e-residents and non-residents. Very often, a virtual currency service provider with an activity license issued in Estonia is only associated with Estonia by registration. Actual business operations, board members, beneficial owners, and also customers are located abroad. All this renders difficult supervision and processing of cases with necessary elements of a criminal offence. At the same time, the large number of companies with an activity license brings about a high risk of reputational damage for Estonia and there is no practical benefit for the Estonian state in hosting companies with activity licenses in its register. Due to the above, exploitation of virtual currency service providers in criminal schemes became commonplace and Estonia began to receive hundreds of foreign inquiries from other FIUs or law enforcement agencies, requesting information to identify and prove criminal offences committed by companies registered in Estonia.

3.1.3. List of national and international areas of activities related to money laundering, including statistics and approaches to prevent such activities

In Estonia, several different agencies are competent to prevent, detect, and combat money laundering, and their activities concern legislation, state supervision, and implementation of criminal proceedings. Within their respective spheres of competence, these bodies also participate in international cooperation.

Ministry of Finance

As a policy maker in the field, the Ministry of Finance also manages Estonia's participation in shaping EU law in the field of money laundering and terrorist financing prevention. The Ministry of Finance participates in the MONEYVAL Estonian delegation and is the contact point for general issues of international cooperation.

Ministry of Justice

The Ministry of Justice is a government agency that performs functions arising from the law and assigned by the Government of the Republic on the basis of law in its area of government. The Ministry of Justice is responsible for planning and implementing national legal and criminal policy, coordinating legislative drafting, drafting the full texts of legislation, processing requests for mutual legal assistance, issues related to courts of first and second instance, prosecutor's offices, prisons, court registers, forensics, notaries' offices, civil enforcement, sworn translation, bankruptcy proceedings, legal assistance, and data protection as well as coordinating crime prevention and preparing corresponding draft legislation in line with the Ministry's competence.

Ministry of the Interior

The Ministry of the Interior is a government agency that performs functions arising from the law and assigned by the Government of the Republic on the basis of law in its area of government. The Ministry of the Interior is responsible for organising activities related to national internal security and public order, planning and coordinating of development, and drafting of corresponding legislation.

Prosecutor's Office

The Prosecutor's Office is a government agency under the Ministry of Justice that participates in the planning of surveillance activities required for the prevention and detection of criminal offences, conducts pre-trial criminal proceedings, ensuring the legality and performance thereof, represents state prosecution in court, and performs other statutory tasks.

Police and Border Guard Board

The Police and Border Guard Board is a government agency under the Ministry of the Interior. The Police and Border Guard Board is a police agency whose purpose is, among other things, to prevent the offences provided for in the Penal Code, process offences, and enforce punishments on the grounds and pursuant to the procedure prescribed by law.

Estonian Financial Supervision Authority

The Estonian Financial Supervision Authority is an institution at the Bank of Estonia (Eesti Pank) with autonomous competence and its own budget, the tasks and competence of which are determined by the Financial Supervision Authority Act and the Money Laundering and Terrorist Financing Prevention Act as well as several other acts.

The Estonian Financial Supervision Authority, as a financial supervisory authority, is involved in the prevention of money laundering foremost though auditing financial intermediaries under its supervision. The task of the Financial Supervision Authority is to check that the organisation and risk management of banks and other financial intermediaries have in place processes and systems that correspond to the relevant business strategy and risk appetite, and are adequately staffed. This includes granting credit, provision of payment and investment services, insurance risks, and wider organisation of financial intermediaries. The Know Your Customer principle is a part of risk management and compliance with this principle constitutes a barrier to money laundering.

Financial Intelligence Unit

The Financial Intelligence Unit is an independent government agency under the Ministry of Finance, which operates on the basis of the Money Laundering and Terrorist Financing Prevention Act and exercises supervision over entities listed in the Act. Obliged entities are obligated to report transactions where money laundering or terrorist financing is suspected and the FIU collects, registers, processes, and analyses this information. During the above activities, it is checked whether information sent to the FIU is relevant for the prevention, detection, or investigation of money laundering or related crimes as well as terrorist financing. If the information is found to indicate a

criminal offence, it will be forwarded to the investigative body for a decision on the institution of criminal proceedings. In addition, the FIU supervises compliance with the requirements of the Money Laundering and Terrorist Financing Prevention Act in respect of companies with an activity license issued by it. In addition, companies become obliged entities in relation to the FIU if certain conditions are met (e.g. traders if they settle in cash for transactions exceeding 10,000 euros; real estate agents as relating to user transactions if the transaction amount exceeds 10,000 euros per month, etc.). The FIU also issues activity licenses to bodies operating as financial institutions, providers of trust and company services, pawnbroking service providers, virtual currency service providers, bodies buying-in and wholesalers of precious metals and precious metal articles or precious stones.

3.1.4. Conclusions

No systemic shortcomings or threats were identified for specific sectors on the basis of criminal statistics and court decisions of the 2017-2019 time period analysed during the implementation of the Risk Assessment. Court rulings that have taken effect have not established that specific sectors are systematically exploited in perpetrating money laundering. Although companies, among other things, have been used to commit money laundering, it is not possible to state categorically that certain sectors of companies or legal persons are exploited systematically. Nor does mere transfer of money acquired from the perpetration of a criminal offence from a personal account or a legal person's bank accounts give reason to claim that credit institutions are systematically exploited.

It is also important here to note that as compared to the legal framework in force at the time of the previous Risk Assessment, both Estonian national law and international standards, including the European Union's directives concerning the fight against money laundering, have changed significantly.

At the same time, certain potential threats or risks can be highlighted. The likelihood of money laundering and the magnitude of its potential consequences may depend significantly on the sector, the impact and extent of its activities in the country, the cash flows, and users of relevant services, including their number, location, and residency.

In view of the above and considering the potential risks, the probability of money laundering can be considered the highest in the financial sector and the financial technology sector. In the case of these two sectors, the consequences of money laundering can also be assessed as higher.

In Estonia, the perpetration of money laundering crimes is mostly detected upon laundering, by way of the Estonian financial system, of the proceeds acquired as a result of crimes committed abroad. In Estonia, persons involved in the perpetration of money laundering are individuals who enable the use of bank accounts of companies or natural persons through which the proceeds acquired by criminal activity are spread across the Estonian financial system or who withdraw cash and return it to criminal offenders. In some cases, the final phase of money laundering has been reached and the laundered assets have been integrated into real estate. Regrettably, as a result of such proceedings, it is not possible to confiscate all assets within the value of the identified proceeds acquired by criminal activity and the value is significantly lower. Although Estonian law also allows individuals to be convicted of committing self-laundering type money laundering, this is somewhat impracticable due to the Supreme Court's judicial practice.

There are innumerable threats as pertaining to how the economic and financial system can be exploited to launder money acquired by criminal activity. Information usually reaches supervision and law enforcement authorities either when suspicious transactions are reported, on the basis of international inquiries, or on the basis of complaints from victims. It is difficult to detect the movement of money acquired by criminal activity where it is necessary to use specific methods of criminal proceedings because frequently the information available is not sufficient to institute criminal proceedings in Estonia. This increases the possibility that the state does not have a clear

understanding or overview of the criminal offences through which, in addition to what is known, money passes through the Estonian financial system and, therefore, information gaps are a threat to efficient prevention of money laundering.

In 2018 and 2019, growing interest of virtual currency service providers in the relevant activity license issued in Estonia was evident. This fast-growing part of the fintech world is, as pertaining to digitally moving values that are measurable in money, anonymous enough to interest criminal offenders. Until March 2020[6], the low control rate of the activity license made it extremely easy for virtual currency service providers to apply for it, and as a result of that the activity license was issued to many that would abuse it as well as to entities providing opportunities to generate and move money acquired from criminal activity. We have seen the results of this in inquiries from foreign countries to Estonia as well as in the constant increase of victims' statements.

In addition to the fact that on the basis of these inquiries and statements it is very difficult or impossible to institute criminal proceedings in Estonia, it has caused a lot of damage to the state's reputation. As a country, we are not sure what these companies do, what kind of customers they serve, and what is the origin of money they move through their companies. This will lead either to high supervision costs or to a situation where the state will have to handle damage caused by hundreds of companies in millions of euros which cannot be reimbursed to the victims. The state itself does not earn anything from activity licensing this segment today because most of these companies do not have operations in Estonia to declare turnover here or employees whose salaries would be taxed or who would boost domestic consumption here, nor do they offer a product/service to the public, the presentation of which would enable Estonia to demonstrate the good reputation of the country.

Table 7. Money laundering threat level at national level

	Money laundering threat level	
National threat level	2.4	**average**

Summary

The national threat level in terms of money laundering is **average** which in turn derives from the fact that the national threat level as pertaining to predicate offences is 1.97, the national geographical threat level is 3.16, and the threat level of sectors included in analyses of this report is 2.29.

3.2. Terrorist financing threat

3.2.1. Nature and extent of terrorist financing threat in Estonia

Terrorist financing is defined as financing or knowingly supporting in another manner of the commission of acts of terrorism as well as making available or accumulating funds while knowing that these may be used in full or in part to commit acts of terrorism. Terrorist financing is also considered to be financing or knowing supporting in another manner of a terrorist organisation or a person whose activities are directed at the commission of acts of terrorism, and making available or accumulating of funds while knowing that these may be used in full or in part to commit acts of terrorism.

Financing acts of terrorism is a criminal offence pursuant to § 237[3] of the Penal Code. The main difference between the nature of terrorist financing and money laundering is that while money laundering presupposes the commission of a predicate offence and the acquisition of property by criminal means, terrorist financing can also take place with perfectly lawfully obtained assets.

[6] Amendments to § 72 of the Money Laundering and Terrorist Financing Prevention Act

In addition, there is a difference in proportions. While in the case of money laundering, causing a serious consequence for the state would presume significantly larger amounts and scales, terrorist financing may also take place by smaller monetary amounts.

In the case of terrorist financing, the purpose of financing is important, which is the commission of acts of terrorism by the relevant person using to that end the assets acquired, in full or in part in the course of terrorist financing. As we can talk about serious consequences in the case of acts of terrorism (see also the definition of acts of terrorism in § 237 of the Penal Code), it also means higher threat assessments in terms of the consequence.

Consequently, legislative tools for combating money laundering and terrorism are similar (rules for obliged entities, the obligation to collect information and cooperate, etc.), but the threat itself and application of the tools is different.

As a result of preparing the National Risk Assessment in 2015, it was found that the risk of terrorist financing is average in Estonia and Estonia could be exploited as a transit country for terrorist financing.

In 2017-2019, no criminal offences relating to terrorist financing, i.e. criminal offences provided for in § 237^3 of the Penal Code, were registered in Estonia.

By its 10 May 2017 Judgment No. 3-1-1-101-16[7] the Supreme Court upheld the 11 May 2016 judgment of Tallinn Circuit Court by which two natural persons were convicted of committing a criminal offence provided for in § 237^3 of the Penal Code.

In Estonia, threats posed by Islamist terrorism are the most likely. Islamist terrorism has been the main security threat in Europe for many years. The resulting deaths and injuries are more expansive than in the case of far-right and far-left terrorist attacks. The activities of terrorist organisations have reached a level where it is no longer appropriate to talk about threatened areas in specific countries; rather, threatened areas now cross several national borders. Terrorist organisations are represented through networks in a number of countries, including Europe. One of the tasks of the networks is to find resources to support terrorist activities.

Calls and campaigns for terrorist financing are being conducted in an increasingly covert manner. Seemingly humanitarian purposes and various alternative funding channels are often used. In addition to alternative payment service providers (e.g. HAW ALA, WesternUnion, MoneyGram, Anelik), channels related to virtual currencies are increasingly utilised. Cryptocurrency is converted into different virtual currencies, and the final recipient's virtual wallet number is usually hidden. It is possible to use various block chain registers to monitor the movement of virtual currency but since the virtual wallet address is not personalised, the efficiency of such registers is almost non-existent.

It is then important to find a systemic solution. The problem stems from technology that is designed to operate anonymously. The solution could be a regulation that would allow only service providers who identify all their customers and counterparties (as banks) to operate legally.

New digital services for electronic payments are constantly emerging, such as virtual currency related services, which are not yet regulated at the legislative level and which make supervision by responsible authorities resource-intensive and complex. Therefore, there is also no complete assurance that their activities are verifiable and transparent. As the seat of many service providers as well as their operations have been transferred outside the territory of the country, it would be necessary to find solutions here as well.

[7] The court judgment is public and available at https://www.riigikohus.ee/et/lahendid?asjaNr=3-1-1-101-16

The use and provision of the relevant service is no longer subject to national jurisdiction. The availability of data from companies registered in other countries and the slowness – and perhaps the impossibility – of responding to inquiries – significantly weaken the efficiency of the fight against terrorist financing. In a situation where control over activities is not guaranteed and activities are not transparent, additional risks emerge.

Virtual currency services that ensure the anonymity of the original users, intermediaries, and persons cashing the money are attractive to the users of money acquired by criminal activity because they are not subject to money laundering prevention rules applied to traditional financial services. In the case of terrorist financing, one cannot and must not rely on limit amounts. Funds are raised in small amounts, in some cases by €10.

3.2.2. Nature and extent of predicate offences to terrorist financing in Estonia

Terrorist financing is not linked to the perpetration of any specific predicate offences. Unlike money laundering, where the criminal origin of assets is significant, terrorist financing can and may take place at the expense of any means, including those obtained through lawful means. Therefore, it is not possible to separately list predicate offences, their nature and the risks associated with them in the case of terrorist financing. Due to the above fact that terrorist financing is not related to predicate offences, they have been assigned the lowest possible threat assessment, i.e. 1.

3.2.3. Nature and extent of international cash flows in Estonia

In preparing this National Risk Assessment, cash flows to and from Estonia in 2017-2019 have been analysed concerning trade in goods, provision of services, direct investments, and remittances.

Cash flows are irrelevant in the context of terrorist financing as small amounts suffice to finance terrorism and, rather, secrecy and anonymity of money transfers is of importance for the financers of terrorism (that is also why persons with criminal intent prefer fintech and cryptocurrency). In addition, statistics is mainly concerned with the so-called public cash flows and movements. As the purpose in the case of terrorist financing is to conceal the movement of money and the fact of terrorist financing, they are not reflected in official statistics.

Based on publicly available statistics, it is not possible to conclude that there has been a movement of cash flows suspected of terrorist financing between Estonia and various countries, including potential risk countries.

As mentioned above, it must be emphasised once again that funds may be raised in small amounts and that virtual currencies may also be used.

3.2.4. Nature and extent of cross-border terrorist financing in Estonia

The implementation of anti-money laundering due diligence measures in the public financial sector and the country's ability to fight terrorist financing have an important impact on the assessment of the geographical threat of terrorist financing. The spread of terrorism around the world affects a large number of countries in Africa, the Middle East, Central Asia, and South-East Asia. Due to networks of terrorist organisations in their neighbouring countries as well as in European countries, for example, the number of vulnerable countries has increased, and use of cross-border services has also led to ways to conceal persons making financial transactions. For example, foreign exchange transactions are made in a neighbouring country to the relevant country of residence.

Estonia is at the forefront of developing financial services and offering activity licenses for virtual currency service providers. An Estonian activity license enables one to operate across Europe, while, at the same time, the system of ex-ante and ex-post verification of activity licenses is currently deficient.

3.2.5. List of national and international areas of activities related to terrorist financing prevention

In Estonia, the competent authority responsible for terrorist financing prevention is the Estonian Internal Security Service that cooperates with other Estonian authorities as well as international partners within the limits of its competence.

The FIU analyses notifications received by it and decides on further actions based on them. In the case of suspicion of terrorist financing, the required materials will be forwarded to the Internal Security Service for further analysis and checks. For example, in 2017, 477 notifications were forwarded to the FIU and in 2018, 173 notifications concerning suspicions of terrorist financing. Of these, the FIU forwarded to the Internal Security Service for additional inspection 477 and 169 transactions, respectively, suspected of terrorist financing. The decrease in the number of notifications received by the FIU is a consequence of training and feedback of obliged entities which pointed out that terrorist financing notifications cannot be based only on the transactions of a customer related to a high risk country but must also include another indicator – that of suspicion or unusualness.

3.2.6. Conclusions

Based on the data collected and analysed during the National Risk Assessment, the following can be concluded:

- The threat level of terrorist financing in most domains is low in Estonia, it is average in the traditional financial sector and high in the financial technology sector.
- In the case of sectors, it is possible to provide estimates of the likelihood of terrorist financing in a particular sector.
- Sectors differ depending on their nature, customer base, regional or international activities, or reach, and the sector's turnover and cash flows. It is important to note here that fintech (and especially crypto) risks stem from anonymity and weaker control over customers and transactions as compared to traditional banks.
- On this basis, it can be concluded that the level of threat is higher in the financial and financial technology sectors and these sectors are more likely to be used for terrorist financing.

As terrorist financing constitutes a criminal offence that consists of financing the preparation or perpetration of acts of terrorism or in the provision of means in another manner, it is important as pertaining to the consequence to rely on the definition of acts of terrorism. Pursuant to § 237 of the Penal Code, an act of terrorism is the commission of a criminal offence against international security, against the person or the environment while posing a threat to life or health, against foreign states or international organisations, or of a criminal offence dangerous to the public, or manufacture, distribution or use of prohibited weapons, illegal seizure, damaging or destruction of property to a significant extent, or interference with computer data or hindrance of the functioning of computer systems as well as threatening with the commission of such acts, if committed with the purpose of forcing the state or an international organisation to perform an act or omission, or seriously interfering with or destroying the political, constitutional, economic or social structure of the state, or seriously interfering with or destroying the operation of an international organisation, or seriously terrorising the population.

By reference to the definition and nature of acts of terrorism, it can be concluded that as pertaining to the consequence, the threat should be assessed as very high.

With regard to the level of geographical risk and cash flows, it can be pointed out that the threat level is higher as pertaining to certain risk countries and conflict areas. Risk countries are considered to be those in which areas controlled by Islamist terrorist organisations or militant units are located, which have an Islamist regime, or where fundamental Islam is widespread.[8]

Table 8. National terrorist financing threat level

	Terrorist financing threat level	
National threat level	2.17	**average-low**

Summary

The national threat level in terms of terrorist financing is **below average** which in turn derives from the fact that the national threat level as pertaining to predicate offences is 1, the national geographical threat level is 3.01, and the threat level of sectors included in the exercise is 2.28.

[8] Estonian Internal Security Service 2019 Yearbook