Estonian Internal
Security Service

Annual Review
2025 ·2026

CONTENTS

Photo: Tiit Blaat

Dear reader,

This year marks the 35th anniversary of Estonia's restored independence and the re-establishment of the Estonian Internal Security Service (KAPO). From a security perspective, the Estonian state and society have faced a range of evolving threats during this time. We have confronted these challenges together, learned from them and grown stronger. These decades of addressing diverse security challenges have provided us with invaluable experience, shaping KAPO into a capable institution prepared to meet today's demands. We recognise that security is complex and interconnected. In addition to a strong military defence, Estonia requires effective internal security, functional institutions, the rule of law and an informed society. In a country that values freedom, all of this is built on trust.

The overall threat picture has not changed. Estonia's principal adversary remains the same – it was, is, and for the foreseeable future will continue to be Russia with its imperialist mindset.

Authoritarian states seek to influence and divide democratic societies, undermine trust in public institutions and weaken countries' resilience and decision-making capacity. A state weakened from within is easier to break. Estonia's experience and historical memory help us understand these dangers. Our society knows and remembers what it means to lose one's freedom.

KAPO's mission is to protect Estonia's constitutional order and internal security. But we do not live or operate in isolation – developments in the world affect us and our sense of security. Threats to Estonia's internal security largely stem from a volatile external environment. This makes today's threat landscape diverse and multilayered. Alongside Russia's continued aggression against Ukraine and other military conflicts, non-military threats are increasingly prominent.

Actors pursuing hostile objectives typically operate covertly. Countering external influence operations is one of the primary battlefields for Estonia and its allies. The adversary seeks to undermine social cohesion and alliances and to erode trust in the state. Sanctions have curtailed Russia's hostile activities, including its propaganda efforts. Much of this activity has shifted to social media, where it is amplified by artificial intelligence and algorithm-driven information flows. Efforts focus on persuading individuals to present hostile narratives as their own, because propaganda is more effective when disseminated by local voices. Last year, we repeatedly saw attempts to destabilise Estonia's internal stability through simple and inexpensive social media campaigns – from bomb threats to attacks targeting the local community in Narva, both on Telegram. For the adversary, having such campaigns amplified by mainstream media is considered a success, as it enhances the credibility and reach of hostile messages. Similar attacks are likely to continue.

We continue to regard the active operations of Russian intelligence services across various environments as a major threat to Estonia's security. We see attempts to recruit individuals at the Estonian–Russian border, campaigns on social media to enlist so-called one-off collaborators, and sophisticated cyber intrusion attempts targeting public- and private-sector systems. Last year, we detected a record number of individuals acting on behalf of Russian intelligence services and expelled foreign nationals who posed a security threat. This does not indicate an increase in the threat level; rather, it reflects the preventive effectiveness of Estonia's internal security efforts.

As a result of KAPO's consistent countermeasures, Estonia does not provide fertile ground for violent ideological or religious extremism or terrorism. The threat posed by far-right and Islamist extremism remains low.

Nevertheless, we must remain vigilant to prevent conflicts in the Middle East, ideological extremism and a broader culture of violence in our interconnected world from spilling over into Estonia. There are no terrorist organisations operating here, but we must be vigilant in preventing attacks by individuals who have become radicalised or influenced by extremist views online. Social media serves as a catalyst in normal-

ising violence, particularly attracting and influencing young people. Major social media platforms could take meaningful steps to limit harmful content, yet short-term commercial logic often leads them to do the opposite.

Ensuring economic security and preventing corruption are becoming ever more important. The state is investing increasing resources in defence and energy, which heightens the need for effective risk mitigation in these sectors. Together, we must ensure that society receives the best value from these investments.

KAPO works every day to make Estonia a difficult target and to make sure people feel safe in the country. In collaboration with domestic and international partners, we maintain a sufficiently strong protective framework to address these threats and challenges. We also provide support to our allies whenever our expertise, capabilities and resources allow. The restrictive and isolating countermeasures and sanctions applied by KAPO, the Estonian state and Europe more broadly against Russia are effective and help safeguard Estonia's internal security. I want to emphasise that sanctions – a means of compelling an end to the war – work. The war in Ukraine has not ended, but we have slowed the momentum of Russia's war machine.

We greatly value and appreciate the contributions of the people of Estonia, citizens of other countries, partner institutions and allies. A secure state relies on an informed and resilient society. Individuals who notice suspicious activities, critically assess information, avoid spreading hostile narratives and report potential threats make a vital contribution to Estonia's security.

Trust within the state and society is one of the most effective protective layers against potential threats. This annual review provides an overview of the threat landscape and the most effective ways to mitigate it.

This is our 28th annual review.
I wish you an informative read.

Margo Palloson
Director General of the
Estonian Internal Security Service

DEFENDING THE CONSTITUTIONAL ORDER

The expulsion of Kremlin-linked activists has significantly reduced Russia's ability to conduct influence operations in Estonia.

Sanctions have curbed Russia's efforts to pursue its politics of division in Estonia, despite more aggressive propaganda on social media.

Entry bans were imposed on seven Russian clergy linked to the Estonian Christian Orthodox Church to reduce the security risk to Estonia posed by the Russian Orthodox Church.

Sanctions have significantly constrained Russia's hostile and propaganda activities, which have now shifted largely to social media. These activities aim to undermine cohesion in Estonian society, weaken relationships with allies, erode public trust in the government and thereby advance Russian foreign policy objectives. One tactic involves amplifying existing divisions within society and creating new conflicts.

In the run-up to socially significant events such as the Latvian parliamentary election this autumn and the Estonian parliamentary election in spring 2027, hostile influence activity in the region is likely to increase.

Russian intelligence services maintain a persistent interest in foreign elections. Previous cases show that collaborators have been instructed to gather information, including on politically active individuals such as politicians. We consider visits to Russia by individuals involved in politics to pose a security risk, as they inevitably attract heightened attention from Russian intelligence services.

The case of Igor Lobin illustrates the interest of Russian intelligence services in utilising politically active Russian-speaking individuals for intelligence and influence operations. In September 2025, Lobin was convicted of conducting intelligence activities against Estonia and sentenced to five years in prison. Under his leadership, representatives of several organisations linked to Russia's politics of division ran in the local elections in Narva in 2017 and 2021 under the electoral list Patriot, but failed to secure any seats.

Social media remains the most cost-effective way to spread and amplify narratives. While European Union sanctions have limited access to major Russian state channels that disseminate hostile propaganda, the continued sharing of this content on social media remains a significant concern. Social media platforms have substantial opportunities to prevent toxic Kremlin video content from reaching wide audiences. Additionally, European Union member states could enforce sanctions more rigorously.

Russia's desire to tighten control over social media content is reflected in its recent restrictions on popular platforms such as Telegram and WhatsApp. The Kremlin is actively trying to steer citizens towards state-controlled Russian applications. Additionally, Russia has restricted

access to YouTube and banned Meta-owned platforms. As a result, users within Russia's information space are likely to receive increasingly censored news, distorted information and manipulated narratives. These include claims of alleged persecution of Russians in Estonia, assertions that Western rearmament is aimed at attacking Russia and misrepresentations of Russian military operations on the Ukrainian front.

Russia also seeks to promote its interpretation of events to the wider world through other methods. Sustaining narratives requires constant repetition, and traditional messaging through Russian state television channels continues. Older audiences rely on these channels far more than on social media. Despite declining viewership, Russian state television maintains its influence, as older Russian-speaking audiences continue to shape attitudes within their communities.

Russia seeks by all available means to promote and amplify narratives portraying Russians as victims and the West as fascist. These narratives are used to justify the ongoing war against Ukraine and to discredit European countries and realistic interpretations of history. In addition, artificial intelligence is used to translate and amplify propaganda narratives automatically. By training language models, the aim is to saturate the internet with content aligned with Kremlin positions, ensuring that the growing user base of chatbots receives responses consistent with those narratives.

'It is time to move towards the greater motherland. Let us get to work!'[1]

Freedom of expression and freedom of the press cannot be regarded as absolute where they conflict with national or international law or threaten the security of the Republic of Estonia. Under a Council of the European Union regulation, it is prohibited to provide support to individuals subject to sanctions.

Russian online portals are used as weapons in the information war, which forms a key component of the Russian Federation's aggression. For Moscow, the media is a tool to construct narratives, spread hatred, create panic and incite hostility.

After the closure of Rossiya Segodnya's Estonian branch, Burceva began working for Baltnews, an online outlet belonging to the Rossiya Segodnya media group. Fearing the same fate as Sputnik Estonia employees Yelena Cherysheva and Allan Hantsom, she used the pseudonym Alan Torm.

Burceva wrote articles aligned with Russia's foreign and security policy objectives, aimed at dividing the societies of Estonia and other countries considered to fall within Russia's sphere of influence. She did so on behalf of a sanctioned propaganda apparatus of a foreign state.

Burceva received assignments from Baltnews deputy editor-in-chief Aleksandra Pavlova, who provided instructions and specified the required tone. Over the course of a year, numerous articles were published that consistently repeated Russian propaganda narratives: "Estonia is a Russophobic state", "Nazism is glorified in Estonia", "Estonia does not uphold the rule of law", "Estonia is not sovereign but acts on Western instructions", "Estonia is a failed state", "Russians are persecuted in Estonia", "History is being rewritten in Estonia", "There is no press freedom in Estonia", "The West is responsible for the war in Ukraine", "Ukraine is governed by a Nazi regime" and similar claims.

In November 2022, Burceva wrote to Pavlova: "I serve Russia."

[1] The following account is based on materials presented at public court hearings; the conviction has not yet entered into force.

Restricting hostile influence activity

Dmitri Kiselyov has been included on the European Union's financial sanctions list as a central figure in Russian government propaganda who supports the use of Russian armed forces in Ukraine.

Kiselyov heads the Rossiya Segodnya media group, which is funded from the Russian federal reserve. The group includes the media outlets Sputnik and Baltnews, which disseminate pro-Kremlin propaganda and disinformation about Russia's war of aggression against Ukraine, portraying Ukraine as a Nazi regime and spreading false claims about a Ukrainian biological weapons programme. They also circulate disinformation alleging that Western countries bear responsibility for the food crisis in Africa as a result of the sanctions they have imposed. Through its influence activities, Rossiya Segodnya attacks Ukraine's territorial integrity, sovereignty and independence, and it supports the annexation of Crimea.

Burceva worked for MIA Rossiya Segodnya, led by Kiselyov, until the end of 2023.

Training of an information warrior

In 2019, Burceva enrolled in the master's programme "Information Conflicts and Hybrid Conflicts" at Sevastopol State University in occupied Ukrainian territory. The programme implements a key state directive issued by President Vladimir Putin to train specialists in information and hybrid warfare. Candidates were recruited through a public video link broadcast from the Rossiya Segodnya press centre.[2] During the programme presentation, Russian State Duma deputy Dmitri Sablin told Svetlana Buceva, in response to her question, that the aim of the programme was to "become a soldier, an information warrior".

The online event was moderated by Viktoria Fyodorova, head of Rossiya Segodnya's press centres.

The master's programme is led by Andrei Manoilo, professor and head of the Department of Russian Politics at the Faculty of Political Science of Moscow State University, who acts in the interests of the FSB. Manoilo is a graduate of the Faculty for Senior Staff Training at the FSB Academy. He is the founder and president of the Russian Association of Information Operations Specialists and a partner in the private intelligence company R-Techno. The company's primary task is to systematically train personnel to plan and conduct information and hybrid warfare operations, creating a reserve force for Russia's information war.

Manoilo's partner and the founder and head of R-Techno is Roman Romachev, an FSB reserve officer and a lecturer in the master's programme at Sevastopol State University. Romachev directed and supervised Burceva's hostile activities against Estonia. They communicated via the messaging applications VKontakte (VK) and Telegram. For example, Romachev instructed Burceva to draft an analysis titled "Europe's Deindustrialisation", describing it as

[2] https://pressria.ru/20190606/952378643.html

an important state assignment. He instructed her to adopt a negative tone regarding Europe's future development: "Europe is fucked!", "The forecasts are bleak". Romachev promised payment for the commissioned work. Burceva did not complete the analysis.

They also agreed to meet in Moscow, but at the last moment Burceva sent her husband in her place. At the agreed meeting time, she sent a message stating: "The agent is already there."

In 2024, Burceva sent Romachev a New Year's message expressing hope that their plans and projects would come to fruition to their advantage and in support of their shared goals.

'Let this book be a weapon.'

In cooperation with Romachev, Burceva published the book *Hybrid War for the World: Where Its 'Battle of Kursk' Will Take Place,* issued in Russia by Romachev's private intelligence company. The book was distributed mainly in Russia, but also in the Baltic states. It was published under the name L. B. Svet, a pseudonym coined by Romachev and presented as the book's author, because Burceva's maiden name was considered too easily traceable by the security services.

The introduction cites Valery Gerasimov, Chief of the General Staff of the Russian Armed Forces, and outlines the so-called Gerasimov Doctrine, which describes shaping the information and psychological environment of an entire population as a central objective in the preparation and conduct of warfare. The book portrays Russia and its allies as targets of attack and accuses Western countries of waging full-scale war across all domains: the information front, the economic front and the social-civil front. It is dedicated to hybrid war for global domination, which, according to its argument, Russia must ultimately win.

On the book's cover, the author was originally described as follows: "The author is a highly classified Russian intelligence officer who, even before the collapse of the Soviet Union, found himself in a foreign land, in a European country, and from afar observed the complex geopolitical processes unfolding in his Homeland. As a true Russian, he naturally experienced the developments in his Homeland with deep anguish. He found himself caught up in forces engaged in a hybrid war against his Motherland."

In passages relating to Estonia, the expression "Soviet occupation" appears consistently in quotation marks. The Republic of Estonia is portrayed as a Russophobic Nazi state that violates human rights,

'It is time to move towards the greater motherland. Let us get to work!'

These were the words written by Estonian citizen Svetlana Burceva to a former officer of the Federal Security Service (FSB) of the Russian Federation while studying information and hybrid warfare in occupied Crimea.

suppresses freedom of speech and is governed by a mentally unstable leadership. These are classic Russian propaganda narratives.

In her correspondence with Romachev, Burceva expressed satisfaction with the book's argument that Russia, together with other so-called sovereign states – a grouping that does not include Estonia – must prevail in the ongoing hybrid war. Dates have long held symbolic importance in Russian influence operations. The book was completed on 9 May, the day Russia commemorates the end of the Second World War. After sending the manuscript to Romachev, Burceva declared, "Let this book be a weapon."

On 9 October 2025, the Tallinn Circuit Court upheld an earlier judgment of the Harju County Court. The lower court had sentenced Burceva to a cumulative term of six years of imprisonment for violations of international sanctions and treason.

The judgment has not yet entered into force. On 19 November 2025, Burceva lodged an appeal in cassation with the Estonian Supreme Court, seeking acquittal.

The Russian Orthodox Church

Russia's aggression against Ukraine and its influence operations during Moldova's 2025 parliamentary election demonstrate how religion has become an instrument of the executive branch in Russia. The activities of the Russian Orthodox Church (ROC) leave little doubt that the church cooperated with Russia's security authorities during the preparatory phase of the aggression and continues to do so during the conduct of the war and the annexation of occupied territories. Cloaked in clerical robes, the Kremlin abuses the argument of religious freedom to undermine security and public order in democratic societies.

The Estonian Christian Orthodox Church (ECOC), which is subordinate to the Moscow Patriarchate and formerly known as the Estonian Orthodox Church of the Moscow Patriarchate, continues to maintain ties with Moscow. In 2025, the church adopted a new name and introduced cosmetic amendments to its statutes to create the appearance of independence from the Patriarch, who persistently justifies Russia's war of aggression against Ukraine using Christian rhetoric. The ECOC continues to be led remotely from Russia by Metropolitan Yevgeny, who was forced to leave Estonia after the authorities declined to extend his residence permit on security grounds.

Although the ECOC presents itself as independent and self-governing, its activities are in fact overseen by the ROC. Guidance and coordination are primarily provided in the name of Vladimir Gundyayev (Patriarch Kirill) by the ROC's Department for External Church Relations and the Administration for the Affairs of Dioceses in the Near Abroad, established on 24 March 2022 – one month after the start of Russia's full-scale war against Ukraine. Such structures closely mirror those of the Russian executive authorities. Their existence also reflects Moscow's continued view that the Baltic states belong to Russia's so-called "near abroad". The close interweaving of state power, intelligence services and the ROC was further illustrated by a statement issued on 12 January 2026 by Russia's Foreign Intelligence Service (SVR), which claimed to defend Orthodoxy in the Baltic states from the activities of the "anti-Christ Patriarch of Constantinople".

In 2025, Estonia declined to extend the residence permit of Mikhail Sorokatyi (monk-priest Ilya), a Russian citizen and cleric of the Narva Diocese of the ECOC under the jurisdiction of the Moscow Patriarchate, who had engaged in divisive activities and historical propaganda in cooperation with the Embassy of the Russian Federation. Sorokatyi arrived in Estonia from a Mordovian monastery in 2013 and took up duties as a monk-priest in the small town of Mustvee. Since his arrival, he has participated annually in commemorative events in Estonia that support Kremlin propaganda narratives. Most recently, in April 2025, he took part in a Russian Embassy propaganda event at the grave of Dmitri Ganin, who was killed during the Bronze Night unrest in Tallinn in 2007. At the event, the embassy accused Estonia of failing to investigate the incident. Russia has made similar accusations since 2007. Sorokatyi left Estonia in 2025.

Long-term residence permits were also revoked for nuns employed by the parish of the ECOC's Resurrection of Christ Cathedral in Narva. In 2025, Igumenia Yekaterina Chainikova, the abbess of the Exaltation of the Cross Jerusalem Stavropegial Convent[3] near Moscow, was employed by the ECOC. The ECOC also maintained an employment relationship with Elvira Koroleva (nun Yuvenalia), the convent's treasurer.

The Exaltation of the Cross Jerusalem Stavropegial Convent is directly linked to supporting Russia's aggression. Some of its nuns collect assistance for the war effort, including fuel and camouflage nets, visit wounded soldiers, and deliver medicines and food to occupied territories. The activities go further. In cooperation with the All-Russia People's Front, overseen by Sergei Kiriyenko, Deputy Head of the Presidential Administration, weapons are also supplied to occupied territories. The All-Russia People's Front was likewise used to interfere in Moldova's elections. As head of the convent, Chainikova supports Russia's aggression in Ukraine in line with the calls made by Vladimir Gundyayev (Patriarch Kirill).

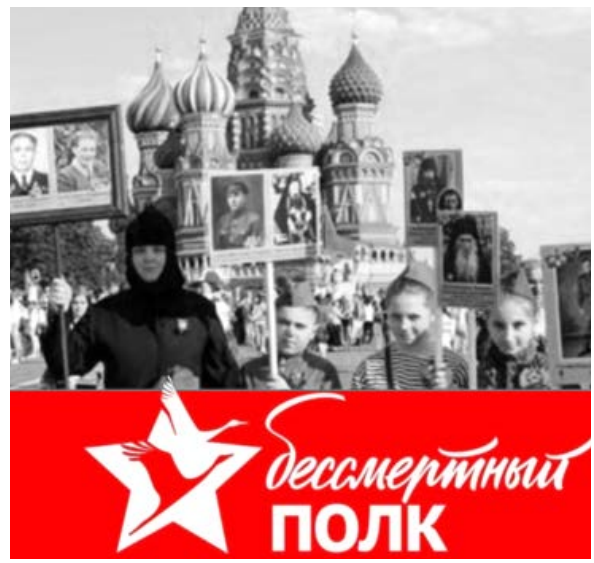
The convent's leadership has openly stated that its support for the aggression followed the Patriarch's appeal, which it regarded as an order from a commander-in-chief. In 2025, Aleksei Shlyakhtin (monk-priest Mark), a cleric of the convent who was employed by the ECOC, also participated in activities supporting Russia's aggression.

In February 2026, Dmitri Burov (monk-priest Daniil), who was associated with the ECOC, left Estonia. Burov refused to answer questions from Estonian authorities concerning the intelligence services and the armed forces of the Russian Federation. He also declined to express his view on Russia's aggression against Ukraine.

Burov arrived in Estonia at the end of 2017 and was assigned to the Narva Diocese, where he was appointed head of the diocese's youth department. He served in various parishes in the Narva Diocese until the summer of 2022, after which he moved to the Tallinn Diocese. From October 2024 until his departure from Estonia, he served at the St Sergius of Radonezh parish in Paldiski.

[3] The term "stavropegial" refers to a religious entity that is directly subordinate to the Patriarch. For example, the Alexander Nevsky Cathedral in Tallinn and the Pühtitsa Convent in eastern Estonia are also stavropegial institutions.

On 18 June 2024, Elvira Koroleva received the Popular Front's medal "Everything for Victory" from Sergei Kiriyenko. Source: VK



Elvira Koroleva in Moscow in May 2020. Source: VK

On 27 July 2013, Burov took part in celebrations at military unit 62231 and stated in a speech: "Today, the church and the army stand together. There are two institutions in which one serves – the army and the church. Today we are together." Source: YouTube

What Burov did not disclose

Between 2012 and 2013, Burov served as head of the Department for Cooperation with the Armed Forces and Law Enforcement Agencies of the Amur Diocese of the Russian Orthodox Church. In that capacity, he cooperated with several units of the Russian armed forces. He blessed military echelons, boosted conscripts' morale and took part in oath-taking ceremonies.

On 27 July 2013, Burov took part in celebrations at military unit 62231 and stated in a speech: "Today, the church and the army stand together. There are two institutions in which one serves – the army and the church. Today we are together." Source: YouTube

While in Estonia, Burov was also involved in an incident in which he and his associate, Vasili Dyatchenko (Archimandrite Vladimir of the Yaransk Diocese of the ROC in Kirov Region), filmed the territory of the Taara Barracks in Võru, located in southern Estonia, near the entrance and outer perimeter. Burov's "pilgrimage" to the Estonian Defence Forces' Kuperjanov Battalion is hardly typical behaviour for a priest. Still, it helps explain his reluctance to answer questions about Russian intelligence services and the war against Ukraine.

Dmitri Burov with a comrade.
Source: Estonian Defence Forces

Dmitri Burov photographing the Kuperjanov Battalion of the Estonian Defence Forces. Source: Estonian Defence Forces

Clergy of the Estonian Christian Orthodox Church subject to Schengen or Estonian entry bans on security grounds

The activities of these clergy, who are affiliated with the Russian Orthodox Church, pose a security threat to Estonia as they support Russia's aggressive foreign policy and its war of aggression against Ukraine.

2025 Mikhail Sorokatyi, Yekaterina Chainikova, Elvira Koroleva, Aleksei Shlyakhtin, Konstantin Korolev, Roman Kolesnikov

2026 Dmitri Burov

Selective assistance by a Russian diplomat

The primary role of a diplomatic mission abroad is to foster relationships between countries while representing and protecting the citizens of the sending state under the laws of the host country.

In August 2025, Estonia declared Russian diplomat Ovik Muradyan persona non grata for exceeding the authority granted under the Vienna Convention on Diplomatic Relations.

Muradyan helped organise and facilitate the payment of legal fees to Urmas Simon, defence counsel for Andrei Andronov, who had been detained on suspicion of anti-state activities. As the funds originated from the Foundation for the Protection and Support of the Rights of Compatriots Living Abroad (also known as Pravfond or the Legal Protection Fund), which is subject to European Union sanctions, Muradyan's involvement exceeded the permissible scope of diplomatic functions under the Vienna Convention. The foundation was established and is financed by the Russian Federation to advance the Russian government's foreign policy objectives. It forms part of Russia's soft-power infrastructure and helps implement the Kremlin's divisive policies abroad.

Through these actions, the Russian diplomat became complicit in the criminal offence of violating international sanctions. Owing to diplomatic immunity, no criminal proceedings were initiated against him.

During the court proceedings, Andronov, while in prison, handed a copy of his indictment to staff at the Russian Embassy. After Andronov met with Muradyan, his indictment was published on a Russian propaganda channel. Muradyan also offered to cover the legal fees of Anton Patrakov, who had been convicted of a crime against the Estonian state. The diplomat did not extend similar assistance to other Russian citizens detained for offences.

COUNTERINTELLIGENCE

Russian intelligence services are attempting to recruit collaborators in Estonia.

Russia organises social media campaigns to recruit 'one-off' operatives to carry out acts of sabotage.

International cooperation among Western security agencies has reached an entirely new level in response to Russia's war of aggression against Ukraine and the sabotage campaigns conducted by its intelligence services in Western countries since the 2010s. These activities initially occurred on a smaller and more covert scale.

Cooperation between European security agencies offers the best opportunity to identify intelligence officers working under diplomatic cover in Russian embassies and to monitor their activities across the European Union. Regular information sharing, combined with Schengen entry bans on diplomats declared persona non grata, helps prevent these individuals from resurfacing in other EU member states. This cooperation also aids in identifying saboteurs recruited by Russia and operating in different countries, preventing their crimes and ensuring that perpetrators are apprehended and convicted.

All Russian intelligence services – the Federal Security Service (FSB), military intelligence (GRU) and the Foreign Intelligence Service (SVR) – serve to sustain the Kremlin-directed authoritarian regime. The FSB maintains control over Russian society by suppressing dissent and repressing the opposition. All three services gather intelligence on the intentions, capabilities and activities of other states and seek to influence decision-making and public opinion abroad through information operations and sabotage campaigns.

Under current conditions, Russian intelligence services primarily operate against Estonia and other neighbouring states through what they call "intelligence from the territory". Intelligence officers collect information without leaving Russia and actively seek to recruit foreign nationals who visit the country. From within Russia, they use social media applications to contact individuals, many of whom have never visited the country or met their so-called partner in person. At the same time, politicians, officials, researchers and business delegations from foreign countries are travelling to Russia in ever smaller numbers.

Russian special services' primary intelligence focus is the military, economic and diplomatic assistance provided to Ukraine by Estonia and other allied countries. This assistance has also been a target of sabotage operations organised by Russian intelligence services, and there have been attempts in countries supporting Ukraine to damage infrastructure used to deliver aid.

Estonian residents and other foreign nationals who visit Russia may be targeted for recruitment by Russian intelligence officers even if they have no access to classified information in their home country. Russian services are also interested in various forms

of non-classified information and in activities that support intelligence operations, such as observing military units and convoys, taking photographs and videos of them, monitoring construction work near border installations, or damaging various types of facilities.

Intelligence activities of the FSB Border Service operational department

In previous annual reviews, we have described the activities of the FSB, GRU and SVR directed against Estonia and the West. In recent years, the FSB Border Service has been particularly active, and we examine its efforts in greater detail in this edition.

The FSB Border Service, among other intelligence units, also collects intelligence on Estonia. The regional branches of the Border Service – known as border directorates – are located in the administrative centres of Russian regions (oblasts) along the country's external border. Sub-units operating in districts (rayons) along the border report directly to them. In addition to units responsible for guarding land and water borders, the FSB Border Service's territorial structures also include operational departments.

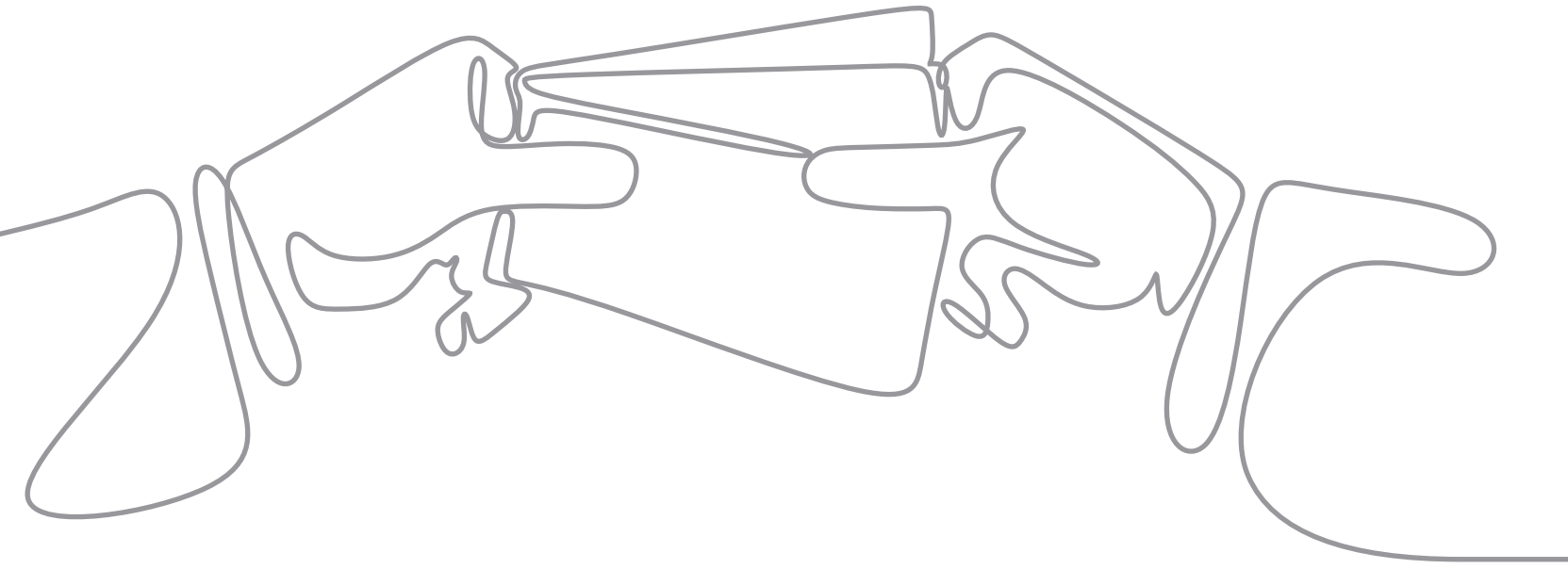
Officers of the FSB Border Service operational departments differ significantly from typical Russian border guards. Unlike the common perception of border guards wearing green uniforms, patrolling the border, or using binoculars and service dogs, operational officers usually work in civilian clothing. They may don uniforms only when necessary to conceal their true purpose. Their main task is to gather intelligence within the border zone and foreign territory beyond it. This includes recruiting informants from among individuals crossing the border and directing their activities. Initial contact with potential agents typically occurs at border crossing points, where officers question travellers about the purpose of their trip, relatives living in Russia and the address of their accommodation during their stay. This information enables the FSB to locate individuals quickly at a later stage. Since the start of Russia's war of aggression against Ukraine, travellers have also been required to state their views on Russia's ongoing "special military operation" in Ukraine.

If border crossers are deemed of interest as potential sources and agree to cooperate, further meetings are arranged on Russian territory at pre-agreed locations. Communication may also happen through social media messaging applications. The meetings always take place away from border crossing points. Officers of the FSB Border Service's operational departments target individuals involved in illegal activities, such as smuggling or transporting sanc-

tioned goods across the border, as well as those associated with organised crime. They also target people who work for, or have personal or professional ties to, Estonian law enforcement agencies or strategically important institutions and companies. This includes family members of law enforcement officials, members of the Estonian Defence League who do not have security clearance and thus face no travel restrictions, individuals linked to Ukraine, Russian-speaking residents in Estonia's border regions, and regular cross-border workers, such as bus and lorry drivers. These officers seek information about developments in Estonia and identify others who could be approached for recruitment. Currently, the Russian border services are particularly interested in issues related to Russia's aggression against Ukraine, Western support for Ukraine and the situation of Ukrainians living in Estonia.

Like many other Russian state bodies, the FSB and the operational departments of its Border Service are affected by abuse of office, including corruption. Recruited sources often submit "intelligence reports" that contain trivial or publicly available information, which handling officers then forward to their superiors. These reports allow officers to demonstrate apparent effectiveness, helping them gain recognition and rewards. Additionally, officers often misappropriate part of the funds intended as payment to informants.

In addition to recruiting Estonian and other foreign nationals, officers of the FSB Border Service's operational departments also recruit Russian citizens, from whom they expect information about developments within Russia, such as cross-border smuggling, corruption, drug trafficking and opposition to the Kremlin. Individuals returning from abroad are expected to provide information on conditions in the countries they visited and on individuals of interest. The operational departments receive assistance from employees of other Russian state institutions and companies, who also help identify potential foreign sources for recruitment.



AGENTS APPREHENDED IN ESTONIA

Erna Moiseyeva

Dual Estonian–Russian citizen
Convicted of conducting and supporting intelligence activities against the Republic of Estonia.
Sentence: three years of imprisonment
Affiliation: FSB

Sergei Filatov

Russian citizen
Expelled from Estonia on 4 June 2025 on security grounds.
Entry ban to the Schengen area.
Affiliation: FSB

Ivan Chihaial

Moldovan citizen
Convicted of conducting and supporting intelligence activities against the Republic of Estonia.
Sentence: six years and six months of imprisonment
Affiliation: GRU

Pavel Kapustin

Russian citizen
Convicted of conducting intelligence activities against the Republic of Estonia, providing false information in a residence permit application and violating sanctions.
Sentence: six and a half years of imprisonment
Affiliation: FSB

Ivan Dmitriev

Estonian citizen
Convicted of conducting and supporting intelligence activities against the Republic of Estonia.
Sentence: five years of imprisonment
Affiliation: FSB

Vyacheslav Yefimov

Dual Estonian–Russian citizen
Convicted of conducting and supporting intelligence activities against the Republic of Estonia.
Sentence: three years of imprisonment
Affiliation: FSB

Igor Lobin

Estonian citizen
Convicted of conducting and supporting intelligence activities against the Republic of Estonia.
Sentence: five years of imprisonment
Affiliation: FSB

Anatoly Privalov

Israeli citizen
Convicted of conducting and supporting intelligence activities against the Republic of Estonia.
Sentence: six and a half years of imprisonment
Affiliation: FSB

Stanislav Matlak

On 20 May 2025, KAPO proposed that the Police and Border Guard Board revoke the residence permit of Ukrainian citizen Stanislav Matlak, who had been working for the FSB. As a result, he was expelled from Estonia and transferred to the Ukrainian law enforcement authorities.

Matlak had been living in Estonia with his family since 2019. Before that, he had worked in both Russia and Ukraine and had travelled to regions of Ukraine that were under Russian occupation. In 2017, the FSB detained Matlak at the Horlivka border crossing point on suspicion of smuggling but released him after questioning. The crossing point lies in an area of Ukraine currently occupied by Russia. In 2023, the FSB re-established contact with Matlak and referenced their previous conversation from years earlier at the Horlivka crossing. This marked the beginning of his covert cooperation with the intelligence service of a hostile state. When contact was re-established, the FSB was unaware that Matlak had moved to Estonia.

Before his detention, Matlak had purchased anonymous SIM cards from Estonian mobile operators on behalf of the FSB and passed the associated numbers to his FSB handler. The handler used the SIM cards to activate accounts on messaging applications, which the FSB then utilised in other operations. Matlak received no payment from the FSB for his services. His motivation stemmed from concern for relatives and property that remained in Russia and in the Russian-occupied territories of Ukraine. He had no moral reservations about cooperating with the FSB.

Matlak communicated with FSB officer Maksim Mishustin, born in 1992, who served in a unit primarily tasked with collecting intelligence on Ukraine and conducting influence and sabotage operations aimed at destabilising the Ukrainian state and society. This unit was responsible for gathering intelligence on Ukraine prior to Russia's full-scale invasion in February 2022 and for preparing the operational environment in the capital Kyiv and in other Ukrainian regions where the Kremlin expected the collapse of Ukraine's legitimate authorities within a matter of days. It has since become clear that the intelligence provided to the Kremlin by Mishustin's unit was false.

Mishustin's name and face have been publicly known since May 2024, when the Security Service of Ukraine (SBU) foiled a plot to assassinate several senior Ukrainian officials, including President Volodymyr Zelenskyy, the heads of the SBU, and Ukraine's military intelligence service GUR. This operation also revealed a Russian agent network operated by FSB officers, which included Mishustin.

FSB officers Maksim Mishustin, Dmitri Perlin and Aleksei Kornev, who were involved in planning a terrorist attack against Ukraine's leadership in 2024. Source: SBU (https://ssu.gov.ua)


ALA
AVATUD
OPEN
ОТКРЫТО
VIDEOVALVE
10
4 h

EXPELLED FROM ESTONIA

Denis Ten

Russian citizen
Posed a threat to the security of the Republic of Estonia.
Maintains contacts with Russian intelligence services.

David Arutyunyan

Russian citizen
Posed a threat to the security of the Republic of Estonia. Engaged in the dissemination of Russian historical propaganda and hostile activities directed at Estonian border officials.

Andrei Zhuravlov

Russian citizen
Posed a threat to the security of the Republic of Estonia. Established contact with a Russian intelligence service and began making preparations in Estonia to carry out further tasks. His expulsion was intended to disrupt the activities of a Russian intelligence service and prevent potentially serious consequences.

Kirill Kudriavtsev

Russian citizen
Posed a threat to the security of the Republic of Estonia.
Maintains contacts with Russian intelligence services.

Source: Delfi Meedia, Ilmar Saabas

Russian Embassy battles the forces of nature

In 2025, pensioners in different regions of Estonia were asked to photograph grave markers and monuments at Second World War burial sites during ongoing reburials. These images were primarily intended to support misleading and hostile narratives against Estonia, as they were used in anti-Estonian influence operations aimed at sowing divisions in society. The head of the Investigative Committee of the Russian Federation, Aleksandr Bastrykin, even opened a criminal case concerning the alleged desecration of grave markers. This action constituted a blatant interference in Estonia's internal affairs.

In its efforts to justify its narratives, the Russian Federation also found itself battling with forces of nature. For example, the Russian Ministry of Foreign Affairs sent a diplomatic note to Estonia's chargé d'affaires in Moscow regarding an alleged act of vandalism at the Defence Forces Cemetery in Tallinn. Reports indicated that 40 war graves were said to have been splashed with red paint. However, an expert assessment established that the discolouration was actually caused by algae growth (a filamentous green alga, most likely *Trentepohlia jolithus*), which is common in Estonia's climate.

‘One-off’ recruitment campaigns

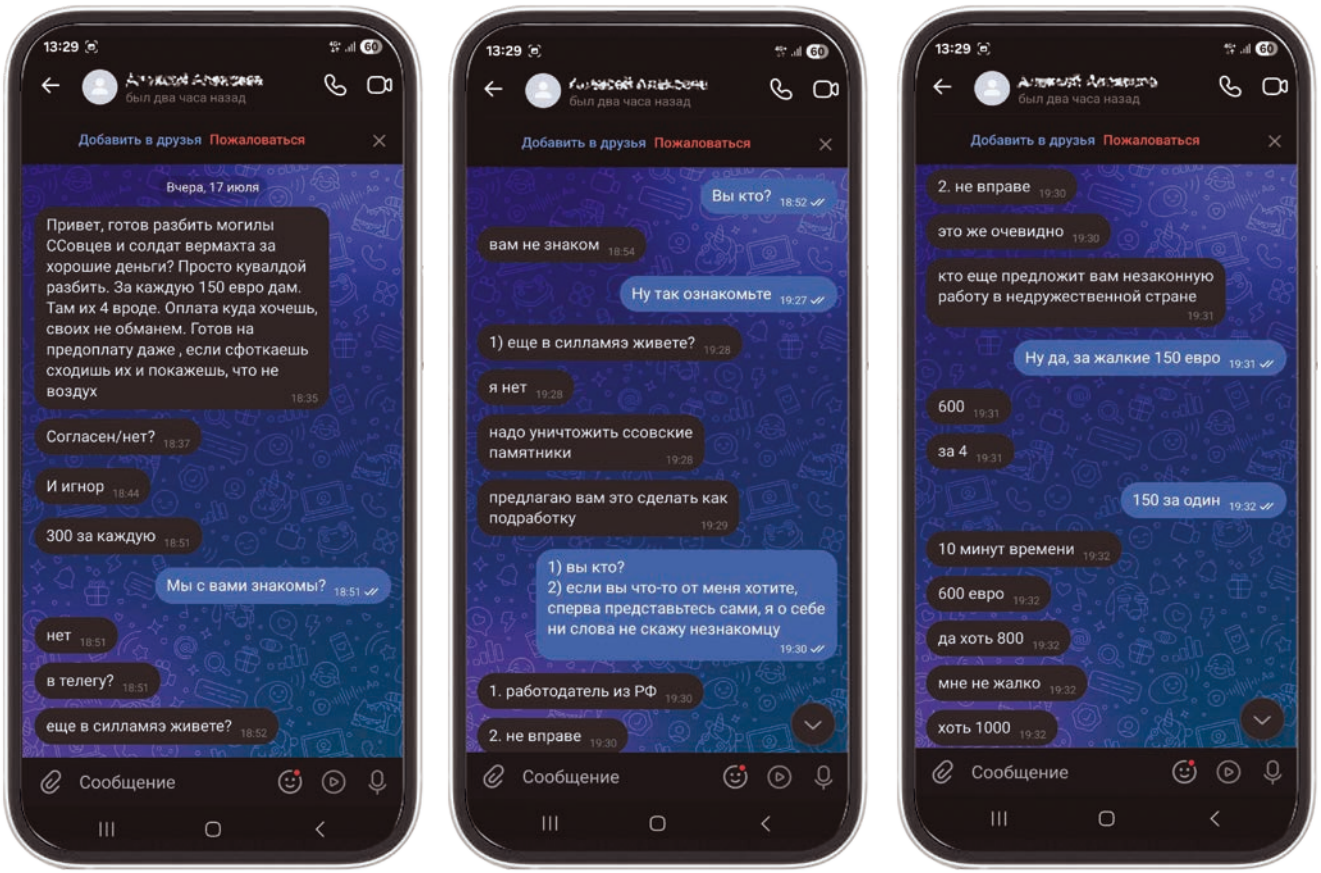
Across Europe, attacks on key public facilities and symbolically significant sites continue. These attacks are typically linked to psychological, political and propaganda strategies. In Russia, the deliberate use of symbols as political instruments is rooted in the country’s political system, historical experience and military doctrine. The Soviet Union built a state propaganda system designed to shape people’s way of thinking. Narrative and information were regarded as effective weapons in their own right, and they continue to be used actively today.

In our 2018 annual review, we described how the Russian Federation uses monuments and memorial sites as tools for influence operations to spread propaganda narratives and inflame social tensions.

These same symbols are still being exploited for these purposes, although the tactics have evolved. In the past, monuments were daubed with paint or covered with flowers; now, “one-off” perpetrators are commissioned to topple and damage them. A social media campaign was launched last summer and autumn to recruit individuals to vandalise the memorial. The monuments at Sinimäed symbolise a painful defeat for Russia in battle and have previously been targeted by Russian intelligence services.

Damaging symbolically significant sites is intended to provoke anxiety and deepen divisions in society. Calls to photograph, film, deface or destroy various sites are ongoing.

In 2025, Russian intelligence services recruited, among others, minors for sabotage operations.



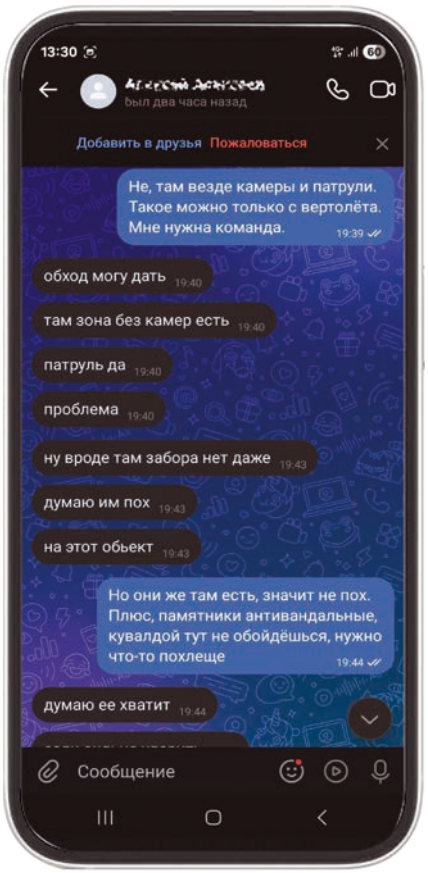
Chat messages seeking to recruit an individual to sabotage monuments. English translations are provided on pages 64–65.

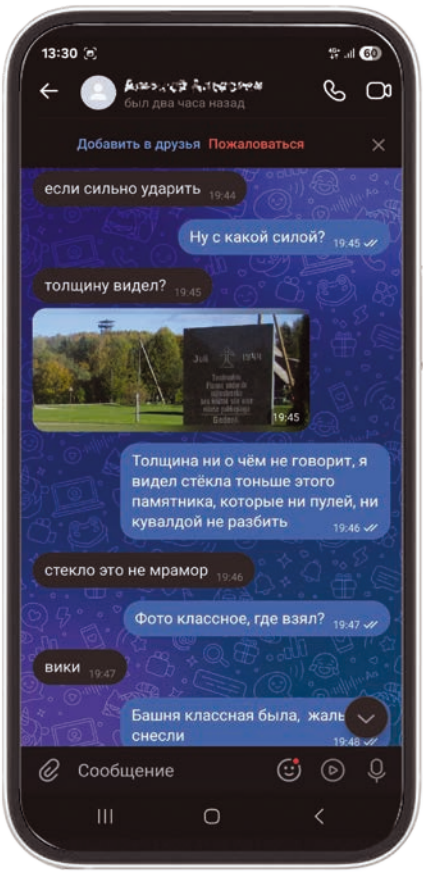
Children are particularly vulnerable, as they may readily respond to calls circulated on social media and agree to damage memorials or other property without understanding the consequences of their actions.

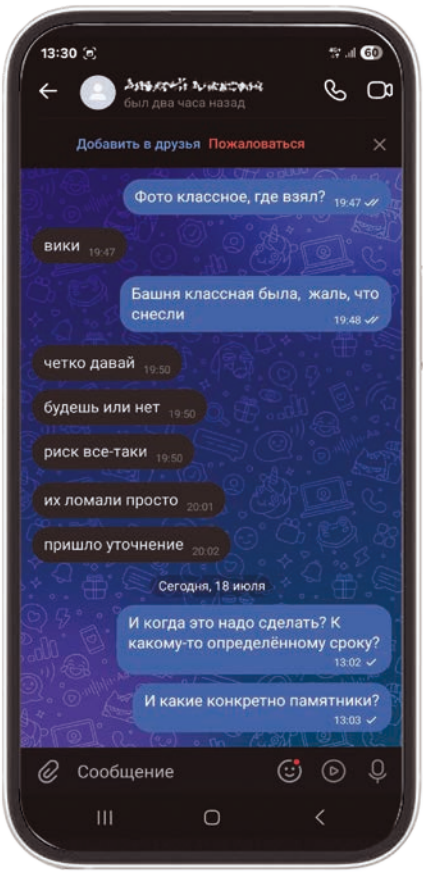
Russia also considers members of the voluntary Estonian Defence League as potential recruitment targets because they do not face the same travel restrictions as members of the Defence Forces. At the end of 2025, a Defence League member in Narva received a Facebook message from someone claiming to represent Russian media, inquiring about the perceptions of Russian-speaking residents in Estonia's border areas regarding the threat from Russia. This was an attempt to establish contact, which the Defence League member duly reported. We commend this responsible action.

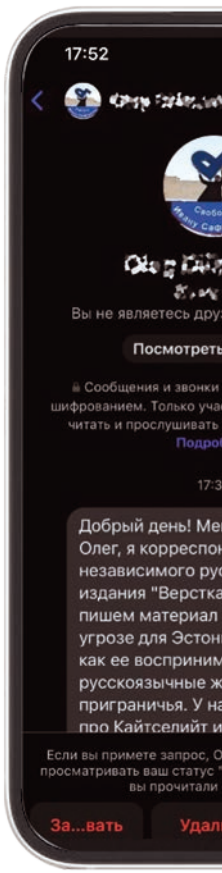
Cooperation with the intelligence services of an aggressor state is illegal. Any payment offered for such activities, if it is paid at all, is minimal. Estonia's law enforcement authorities quickly detect such crimes and bring those responsible to justice. Individuals convicted of such offences must serve their sentences and compensate for the damage caused, which, based on previous cases, typically far exceeds any payment received for their actions.

It is also important to note that Russian intelligence services, which orchestrate acts of vandalism or sabotage, show no concern for the individuals who carry out these tasks once they are arrested. In Russia, they are referred to as "one-offs" – disposable individuals who are discarded once they have served their purpose.









Z symbol

Based on the evidence gathered, Estonian citizen Ivan Pletnyov received a proposal on Telegram to spray the letter Z on three buildings in Estonia. The letter has become a symbol of Russia's aggression against Ukraine. Pletnyov had previously drawn attention for displaying symbols associated with Russia's war efforts and had repeatedly come under the scrutiny of the Estonian Police and Border Guard Board. The graffiti he was asked to create expressed support for, or sought to justify, the Russian Federation's aggression and acts of genocide in Ukraine.

According to the case file, Pletnyov was instructed to vandalise the main building of the Estonian Parliament and the headquarters of the Estonian Defence League. He was not offered payment for these tasks. Evidence suggests that he was interested in obtaining a travel voucher to Russia and naively believed that in exchange for his actions, Russia would provide him with a diplomatic passport and facilitate his travel across the border.

Assisting Russian intelligence services, or individuals acting on their behalf, and maintaining contact with them can lead to a prison sentence of up to 15 years. Additionally, those found responsible must compensate for any damages caused. For citizens of Russia, Ukraine or other non-EU countries, this may also result in expulsion from Estonia and the Schengen area, along with a ban on re-entry.

Syrians as pawns of Russian intelligence

Migration pressure on the Schengen border from the Russian side is not a spontaneous occurrence; it is orchestrated and controlled by Russia's Federal Security Service (FSB), which uses migrants as a tool for exerting pressure on neighbouring countries.

In our 2023–2024 annual review, we described how FSB officers at the border assumed the role of propaganda operatives. In 2025, we identified in greater detail how migration pressure was organised on the Russian side of the border.

In 2023, an FSB handler, with the assistance of an accomplice, arranged for the transport of Syrian migrants from Saint Petersburg to the border zone near Ivangorod. The handler promised the accomplice 10,000 roubles – approximately 100 euros – for transporting the migrants. The accomplice was given an address in Saint Petersburg where, at a specified date and time, he was to pick up the Syrians and drive them to the designated location.

Do not put your future at risk. If you or someone you know is approached with a proposal to damage or set fire to property, refuse and report it to kapo@kapo.ee.

During their journey, the migrants had their personal belongings taken from them. Near Ivangorod, about eight kilometres from the Estonian border, the Russian border zone begins. In the dark, the driver took the men there as agreed and waited for a signal given by torchlight. When a light flickered in the distance, he ordered the Syrians to exit the vehicle and instructed them to walk towards it. He then drove away.

It emerged that, in addition to the Syrians, others had been similarly gathered in the border zone. In a meadow in Ivangorod, an Estonian border post is installed to mislead migrants into thinking they have reached the Estonian border. The migrants were instructed to start walking from there into what they believed would be free Europe.

Before they reached the actual border, Russian border guards emerged from the bushes and informed the Syrians that they were not allowed to stay in the border zone. The group was directed to the border crossing point, and their ordeal on the Narva bridge was filmed. The footage was later used in influence operations and propaganda. After being returned to Russia, the Syrians were instructed to read pre-written statements on camera, stating that Europe had refused to accept them and that they had been mistreated. Their money and personal belongings were confiscated, and they were given false instructions on how to move around within the Russian border zone. Ultimately, they were used for propaganda purposes.

COMMUNIST PARTY OF CHINA: PROPAGANDA IS MORE EFFECTIVE WHEN DELIVERED BY LOCAL VOICES

In 2025, the People's Republic of China expanded and diversified its influence activities, offering Estonians from different backgrounds a curated and polished 'China experience' in culture, media, education and business.

The Chinese Embassy directs, monitors, mobilises and trains the Chinese diaspora to silence dissent and to advance the interests of the Chinese state and its enterprises in global competition for dominance.

China's intelligence efforts focus on research, technology and security. After establishing contact through LinkedIn, Chinese intelligence services attempt to lure influential individuals to China or neighbouring countries. Travel to China creates recruitment opportunities for its intelligence services.

In the People's Republic of China, culture and education fall under the Chinese Communist Party's propaganda system. Under the guise of cultural cooperation, China sends propaganda officials to Europe, including Estonia, to promote the "China story" through cultural engagement and to divert attention from China's human rights abuses, unfair economic practices and its growing support for Russia in the war against Ukraine.

In strategic communication, China assigns significant weight to propaganda. One aspect involves leveraging the economic appeal of China's vast but tightly controlled market. Another, less discussed aspect is the use of China's economic power for political ends – for example, imposing informal sanctions on Australia after it called for an investigation into the origins of Covid-19, and on Lithuania after it withdrew from the 16+1 format and allowed the opening of a Taiwanese representative office.

The overarching objective of the Chinese Communist Party is to achieve military, economic and technological supremacy. Chinese society as a whole, including its intelligence services, has been mobilised to serve the "China Dream" – to become a leading global power with a world-class military by 2049 and the capability to seize Taiwan by 2027.

The Chinese Embassy in Estonia has stepped up cultural outreach to counter China's negative image. A similar trend is visible across the European Union. Numerous cultural events are organised in cooperation with local authorities. Alongside these events, meetings are held with members of the local political and business elite, seen as opportunities to build contacts and shape attitudes towards China. Efforts to cultivate favourable views begin early – the Chinese ambassador is a frequent guest at Estonian schools and universities.

The Chinese Communist Party believes its messaging is more effective when Estonian politicians, cultural figures, academics, experts and journalists speak about their personal experiences of China.[1] To this end, the Chinese Embassy invites Estonian citizens on fully funded trips to China. In 2025, local government politicians, cultural workers, experts, journalists, media professionals and content creators visited China. In October 2025, for example, a delegation of Estonian media representatives travelled to Nanjing and Suzhou at the invitation of the Chinese Embassy. The trip was organised by a foreign affairs company affiliated with the Jiangsu provincial government and included briefings on Chinese history and the technology sector.

[1] https://archive.ph/Q0d8y

Source: Weixin

According to the Jiangsu foreign affairs company, the journalists pledged to share Jiangsu's story with the Estonian public through the media in order to promote cultural exchange and economic cooperation between China and Estonia.[2]

In October, young Estonian experts also visited China to take part in the China–Europe Youth Dialogue in Hangzhou. The dialogue was organised by the Chinese Academy of Social Sciences (CASS), which maintains close ties with China's intelligence services.

As early as 2019, the Chinese Embassy stated that the role of journalists is to promote relations between China and Estonia. In 2025, the Chinese Embassy published several sponsored articles in Estonian and other Baltic media outlets on "democracy", "fair trade" and Taiwan's "historical" status as part of China, even though the Chinese Communist Party has never governed Taiwan. The embassy pays local companies for media and public relations services, which, in turn, connect Estonian journalists with the embassy and secure the publication of favourable content in local media outlets. When dealing with representatives of the Chinese state, it is important to bear in mind that lavish hospitality may carry expectations. China's generous treatment can come at the expense of journalistic freedom and independence.

Culture and media are not the only sectors the Chinese Communist Party seeks to use to advance its goals. Influence operations also target the technology sector. The Estonian-Chinese Chamber of Commerce, established in 2022, has targeted Estonia's technology sector and sent phishing emails to several growth and technology companies, offering lucrative cooperation with China. The proposals were not sent to company executives or general contact addresses but to individuals responsible for technology. The founders of the chamber have also sought to establish contacts with European Union institutions to discuss EU investments, relations with the United States and Asian countries, and other matters. The chamber's activities extend beyond the technology sector.

Mobilising the local diaspora

The Estonian-Chinese Chamber of Commerce is linked to the Chinese Embassy in Tallinn and regularly participates in events organised by the Chinese Embassy in collaboration with Chinese researchers, students and lecturers from Estonian universities. Participants are urged to familiarise themselves with the Party Congress talent strategy's technology transfer programme, strengthen their security awareness while studying abroad, act as "ambassadors" on university campuses and promote the official "China story". In other words, they are expected to advance Chinese propaganda and build a "harmonious" student community. In China, "harmonisation" refers to the censorship of dissent and minorities. Students and lecturers have pledged to integrate their personal development with the broader goal of China's development and national rejuvenation.[3]

In 2025, the use of professional networking platforms, such as LinkedIn, intensified as a means of identifying intelligence targets.[4] A new trend involves posting job advertisements rather than sending personalised messages, and then approaching selected candidates.[5] Particular value is placed on experience in government service and in foreign or security policy. Estonian politicians, diplomats, ministry staff, members of the Defence League and researchers have received cooperation offers.

[2] https://ee.china-embassy.gov.cn/dssghd/202505/t20250527_11634585.htm
[3] https://archive.ph/kR92U
[4] www.bbc.com/news/uk-67142161
[5] www.gov.uk/government/news/action-to-disrupt-and-deter-threats-to-uk-as-mi5-issues-spy-alert

Instead of direct approaches, job advertisements are increasingly used. In November, for example, the United Kingdom's Security Service, MI5, issued a warning to Parliament and its staff about espionage risks linked to Chinese recruiters, citing two LinkedIn accounts. In October 2023, the head of MI5 stated that, in their assessment, nearly 20,000 Britons had been approached on LinkedIn.

China's technological ambitions, including intelligence activities focused on technology, are well known internationally. Chinese law requires citizens and organisations, including those abroad, to cooperate with the Chinese state. As a result, Chinese nationals and organisations cannot refuse a request for cooperation if it is made by the Chinese authorities or intelligence services.

Estonian media representatives who travelled to China at the expense of the PRC. Source: Weixin

CYBERSECURITY

Logging into work environments through shared devices poses a risk.

Russian and Chinese state-sponsored actors conduct phishing attacks against selected government bodies and companies.

Russia's full-scale war against Ukraine has now entered its fifth year, with a significant portion of the country's resources still dedicated to the war effort. In cyberspace, Russian intelligence services are focused on Ukraine and on supporting military operations through cyber means. However, they continue to conduct operations against the West, including Estonia. In Estonia, Russian cyber units show particular interest in all matters related to Ukraine, targeting both the public and defence sectors as well as logistics, transport and industry. It is therefore essential that private-sector actors also recognise cyber risks and implement measures to mitigate them.

Laundry Bear

In May 2025, the Dutch intelligence and security services publicly identified a new Russian state-sponsored cyber threat actor, or APT,[1] which they named Laundry Bear.[2] In Microsoft reporting, the same actor is referred to as Void Blizzard.[3] It focuses on targeting official email accounts and other cloud service accounts of companies and government bodies. As with other Russian state-backed cyber units, its primary interest lies in Ukraine-related matters, as well as broader foreign policy and technology issues. Because the activity primarily involves official email and cloud accounts, a successful intrusion could grant access to sensitive professional information that might harm Estonia and our cooperation with Ukraine and other allies. In addition to government bodies, Laundry Bear targets the defence sector, cultural organisations and digital service providers. A characteristic tactic is the use of stolen passwords. The unit uses all available methods to gain access to accounts, including phishing, password databases and password spraying attacks.

Using stolen credentials, the actor quickly extracts large volumes of emails and files. We have observed attempts by Laundry Bear to carry out password-spraying attacks against the web services of Estonian government bodies.

[1] Advanced persistent threat – a term used in cybersecurity to describe sophisticated, goal-oriented threat actors characterised by sustained and high-intensity activity. Such actors are often state-sponsored.

[2] www.aivd.nl/documenten/publicaties/2025/05/27/aivd-en-mivd-onderkennen-nieuwe-russische-cyberactor

[3] www.microsoft.com/en-us/security/blog/2025/05/27/new-russia-affiliated-actor-void-blizzard-targets-critical-sectors-for-espionage

Recommendations for mitigating cyber threats

Remote work	• Implement two-factor authentication for all users • Use centrally managed work devices • Prohibit remote access without a VPN solution • Grant access rights strictly on a need-to-know basis • Store backups on a separate network drive or server
Shared devices	• Enable automatic logout at the end of each session and clear browser data after every use • Prohibit shared administrator accounts and assign a unique account to each user • Prohibit software installation without administrator approval
Cloud services	• Retain logs for at least one year • Restrict access and implement a zero-trust model, which assumes by default that no user, device or application is inherently trusted
Security vulnerabilities	• Patch vulnerabilities without delay • Replace outdated devices and legacy systems that no longer receive security updates
Supply chain attacks	• Ensure that third-party access is limited and auditable • Stay informed about the security measures used by service providers and clients

Risks of remote work

As services increasingly move to the cloud, the number of attacks targeting cloud services can be expected to grow. The risks associated with cloud solutions and remote working must therefore be mitigated. Using shared devices[4] to access work environments poses a particular danger, as passwords are often stolen from such less protected devices. One common method involves fake login pages that closely resemble legitimate services. When users enter their username and password, attackers capture their credentials. We have also seen passwords leak from public devices, such as library computers. With shared devices, it is often impossible to know which links a previous user has opened or which applications have been downloaded. Malware may run unnoticed and transmit login credentials to criminal-controlled databases.

As stolen passwords are routinely traded, compromised credentials are likely to be misused at some point. Hostile intelligence services use leaked passwords to gain access to sensitive or targeted information. Cybercriminals exploit them for financial gain – for example, by logging into a company employee's account to send partners fraudulent invoices in which the bank details are replaced with accounts under the cybercriminals' control. It is therefore essential to manage the risks associated with remote work and to ensure that access to work environments and internal networks is permitted only from centrally managed devices.

In addition to Russia, China continues to conduct cyber espionage against Estonia. Chinese state-sponsored actors continuously conduct phishing attacks targeting specific government bodies and companies. In 2025, they launched several phishing campaigns targeting Estonian government institutions. In one case, publicly accessible document registers were used to identify individuals who would then be targeted with a phishing email. Carefully selected recipients were then sent a message in fluent Estonian, containing a malicious link. Notably, the email referred to a current issue: the targeted institutions were indeed undergoing organisational changes, which were mentioned in the message. The attack targeting Estonia was detected, and it was unsuccessful. However, similar attempts enabled the attacker to gain access to several institutions and organisations worldwide. Further details on the scope of the campaign can be found in Unit 42's report "The Shadow Campaigns".[5]

Network devices

Network devices remain a target for state-sponsored actors from both Russia and China. They do not distinguish between large and small users: devices belonging to home users, companies and government institutions alike are targeted. Compromised devices are used to gain access to networks, steal data, launch further attacks and conceal malicious activity.

[4] Shared devices also include home computers used by several family members – for example, when a parent uses the same computer for remote work that children use for gaming or schoolwork.

[5] https://unit42.paloaltonetworks.com/shadow-campaigns-uncovering-global-espionage

Main attack vectors and mitigation measures

The methods used in cyber-attacks against Estonia and other countries in 2025 underscore the importance of strong cyber hygiene to prevent intrusions. Robust cybersecurity measures reduce risks stemming both from hostile state intelligence services and from cybercriminal activity.

A malicious email sent to the Estonian Ministry of Foreign Affairs. Similar emails were sent to several other Estonian government institutions as part of the same campaign.

PROTECTION OF STATE SECRETS

Providing false information or concealing relevant data in the security clearance questionnaire or during the vetting interview undermines an applicant's reliability.

Refusal to grant a security clearance does not require proof of actual harm – identifying a risk is sufficient.

Having held a security clearance in the past does not create a legitimate expectation that it will be renewed. Each clearance requires a new risk assessment.

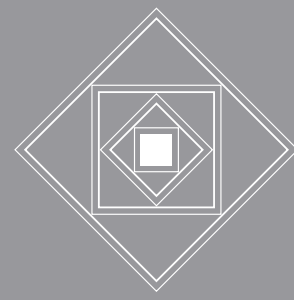
On 30 June 2025, the Estonian Supreme Court[1] dismissed an appeal by an Estonian ambassador who was challenging KAPO's decision not to renew his security clearance for access to state secrets. In 2021, KAPO had refused to extend the diplomat's clearance after security vetting determined that he had deliberately provided false information and concealed relevant data during both the interviews and the renewal questionnaire.

The ambassador challenged the decision in court, claiming that he had not deliberately concealed information and that his hearing during the proceedings was merely a formality. Both the administrative court and the circuit court dismissed his complaint. In the summer of 2025, the Supreme Court's Administrative Law Chamber reached the same conclusion, upholding the main ruling of the Tallinn Circuit Court's judgment while revising its reasoning.[2]

The Supreme Court upheld the circuit court's finding that the applicant had deliberately concealed information regarding his financial activities, including an additional source of income and property located in Russia, and had also failed to disclose in the questionnaires one place of employment and contacts with foreign intelligence services.

The Chamber concurred with KAPO's assessment that if an applicant for access to state secrets acts in bad faith or otherwise violates the requirements of the security vetting process, we cannot maintain confidence in that person's ability to protect state secrets. Any breach of this obligation puts the protection of state secrets at risk.

[1] Estonian Supreme Court judgment of 30 June 2025 in case No 3-21-1337.
[2] Tallinn Circuit Court judgment of 7 June 2023.



Concealment of information. Applicants and renewal applicants for access to state secrets must disclose all relevant information in the questionnaire, as this enables more precise questions during security vetting and the collection of additional data from other sources necessary to decide whether to grant or extend clearance.

Activities and contacts abroad. Relevant and sufficient information must be provided about activities conducted in foreign countries and contacts maintained there.

Additional sources of income. All sources of income must be declared in the questionnaire, regardless of who qualifies as the recipient under the Income Tax Act. If the applicant manages a bank account into which income is paid and uses those funds, this constitutes an additional source of income. Concealing it may be interpreted as a sign of unreliability.

Facility security clearance

In 2020, we noticed a growing interest among companies in managing state secrets outside government institutions, on their own premises, and in participating in public procurements that require access to classified information.1 In last year's annual review, we highlighted that the increasing involvement of Estonian companies in security, research and development projects, as well as related procurements, requires that authorities adapt swiftly to this expanding role of the private sector in classified work. The legal framework governing industrial security also requires revision to establish clear criteria for assessing which companies are suitable to participate in such projects. It is essential for companies to have a clear understanding of their rights, obligations and responsibilities.

Amendments to the State Secrets and Classified Information of Foreign States Act took effect on 1 September 2025. These changes offer companies more flexible options for obtaining a "facility security clearance" to handle state secrets outside state agency premises and to participate in procurements that involve classified information. Previously, securing a facility security clearance for information classified as confidential, or at a higher level, required establishing a dedicated security area. This requirement has now been eliminated.

Category A facility security clearance

A Category A clearance requires the holder to establish a compliant administrative or security area, allowing for the processing of state secrets on immovable or movable property in the holder's possession.

Category B facility security clearance

A Category B clearance means that a legal entity that has undergone security vetting does not operate its own secure processing facilities. Instead, it provides services at the premises of its contractual partners through employees who hold the required personnel security clearance.

The amendment introduced two categories of facility security clearance: Category A and Category B.

A facility security clearance may be granted to:

- a natural person;
- an Estonian public-law legal entity;
- a private-law legal entity registered in Estonia.

KAPO issues a facility security clearance after conducting a security vetting of the legal entity. Both types of clearance can be granted for up to five years. However, there are statutory conditions that must be met when applying for a facility security clearance:

- the legal entity must have been established at least 18 months earlier; and
- the entity must be economically active.

These requirements are necessary for evaluating the company's reliability and associated security risks. It is not feasible to assess a company that was established right before submitting an application for a facility security clearance. Furthermore, from a security vetting perspective, access to an annual financial report is crucial, as it enables an objective assessment of the company's financial position.

European Union and NATO research and development projects, funding programmes and participation by enterprises may lead to the creation of special-purpose subsidiaries or new legal entities for specific projects. In response, the legislature has introduced greater flexibility for handling information classified at the restricted level, aiming to enhance the competitiveness of Estonian companies. In these situations, the two previously mentioned conditions do not apply when applying for a facility security clearance for state secrets classified at the restricted level.

A state fee must be paid for the review of a facility security clearance:

- 6,000 euros for a first-time application;
- 3,000 euros for extending.

To comply with state secret protection requirements, a legal entity must:

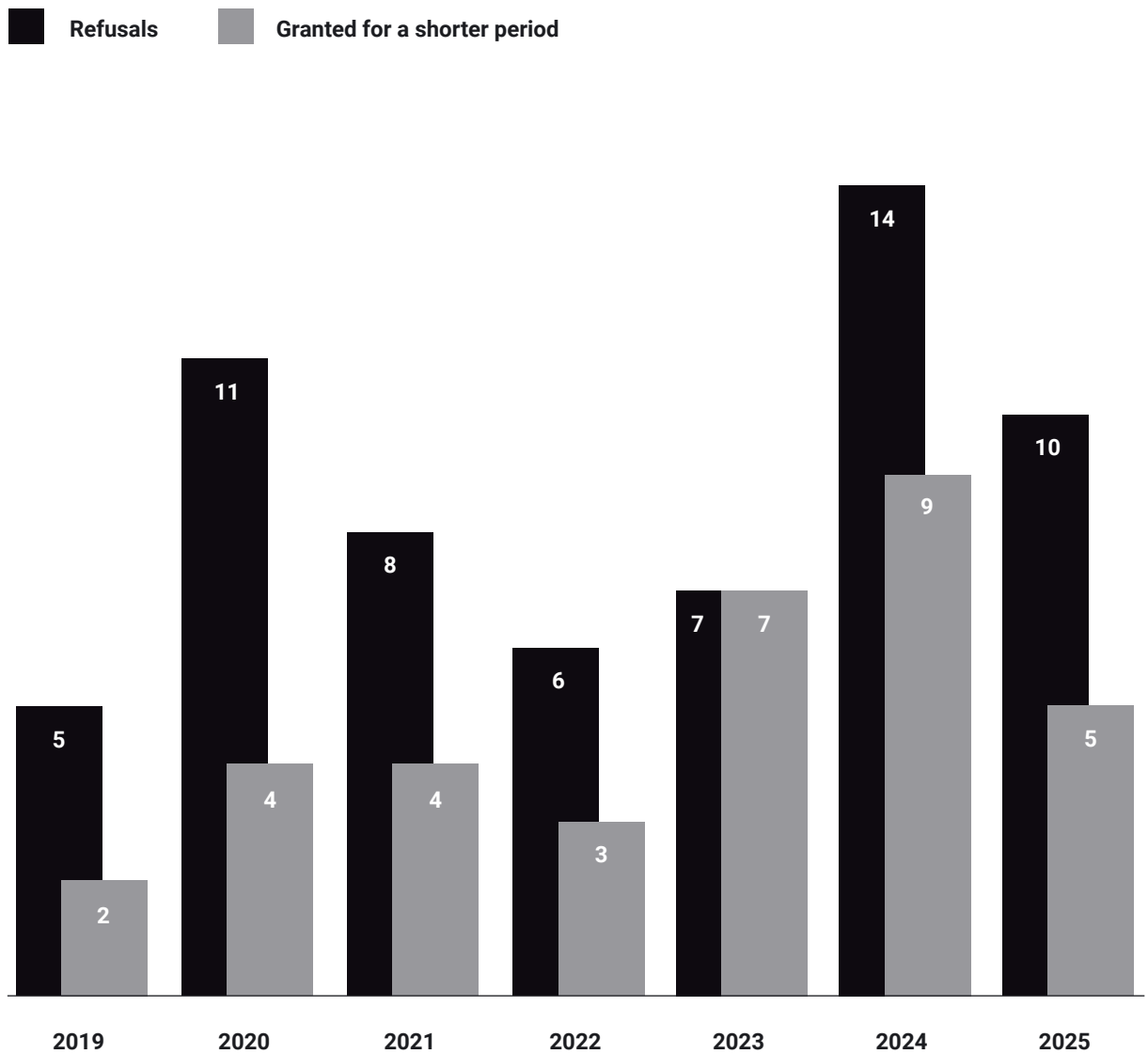
- appoint a person responsible for organising the protection of state secrets. This individual must hold a personnel security clearance at the highest classification level of state secrets processed by the entity; and
- ensure that at least one member of its management body holds a personnel security clearance at the highest classification level of state secrets processed by the entity.

We encourage companies in the defence industry and other enterprises that seek to participate in procurements involving classified information to utilise the new legal options and apply for the type of facility security clearance required for their activities.

Statistics on refusal to grant access to state secrets or granting it for a shorter period than requested

In 2025, the main grounds for refusal focused on established patterns of behaviour or personal habits that could lead to financial dependency. In practice, this primarily included living beyond one's means or difficulties in repaying loans.

In 41 cases, applicants chose to withdraw from the security vetting process, possibly anticipating a negative decision.



PREVENTING AND COUNTERING EXTREMISM

Social media normalises violence, while law enforcement agencies must deal with the real-world consequences.

Radicalisation is occurring at increasingly younger ages through social media groups.

One fifth of the children of immigrants in Estonia do not attend school, which hampers their integration and adaptation to life in the country.

Far-right extremism

The level of extremist threat in Estonia remains low. To maintain this, KAPO has focused primarily on prevention efforts.

The main concern remains with adolescents who feel isolated and find a sense of understanding in international social media groups that promote extremism, where they are exposed to ideologies of hatred and violence. Regular exposure to violent content can normalise violence, and behaviour patterns encountered on social media are carried into real life.

The adoption of extremist views is often linked to social background. Individuals who adopt such views have often experienced trauma related to alcoholism, abuse, neglect and loneliness. Although social conditions are not a direct cause of radicalisation, they create a conducive environment for it. Young people who feel alone in the world seek belonging and understanding in social media groups.

Young people inspired by extremism vary in their profiles. The most visible openly praise extremist symbols and ideology. Others radicalise more quietly – until they join an extremist group on social media.

Violent acts by school-age adolescents can be prevented, and with specialist support these young people can be guided back onto the right path. If a crime has already been committed, or if an adult plans the act, it might qualify as a terrorism-related offence punishable by 5 years to life imprisonment.

Islamist extremism

In 2025, the primary terrorist threat in Estonia came from isolated radicalised individuals rather than coordinated attacks by major terrorist organisations. The nature of the threat has evolved. In the past, Islamist extremists were clearly linked to specific organisations and their ideology was unambiguous. Now, such links are more concealed, ideology is often diffuse, and individuals are not necessarily formal supporters or adherents of a particular terrorist organisation.

Young people radicalise by selectively adopting elements from the ideologies and narratives of different terrorist groups that appeal to them. Violent content is the material most widely consumed online.

Shia extremism

In last year's annual review, we described developments within Estonia's Shia Muslim community, including efforts to establish a separate religious congregation and instances of expressed support for Hezbollah.

Shia Muslims living in Estonia follow religious authorities in accordance with their faith, including Iran's former Supreme Leader Ayatollah Ali Khamenei. Among the more active members of the Shia community are individuals who consume information influenced by Iran's religious leadership and who interpret developments in the Middle East through Iranian narratives.

In 2025, Iran – both directly and through the terrorist organisation Hezbollah, which it supports – carried out terrorist attacks against Jews around the world. In our assessment, those who disseminate or support the ideology of Iran and Hezbollah pose a threat and endanger public order and security in Estonia. For this reason, their residence permits were revoked and the Estonian Police and Border Guard Board, working with KAPO, expelled two individuals who had been in Estonia on study mobility programmes and who were suspected of supporting the terrorist organisation Hezbollah and Iran's Islamist regime.

Terrorist networks operating within the Schengen free movement area may also affect Estonia – for example, through fundraising or the covert movement of individuals.

Kurdistan Workers' Party

Founded in 1978 and operating in Turkey, Iraq, Iran and Syria, the Kurdistan Workers' Party has been designated as a terrorist organisation in Western countries. In December 2023, criminal proceedings were initiated in Estonia against a Turkish citizen of Kurdish origin who had shared a call on social media to join the party. In January 2026, he was convicted by a court in Estonia in a plea agreement and given a suspended sentence of 2 years and 6 months.

Future challenges of integration

Over the past decade, the number of Muslim community members residing in Estonia with a residence permit has increased by more than 5 times.

As the Muslim community grows, so does pressure to establish Islamic kindergartens and schools. Experience in other countries shows that, in some cases, authorities have had to intervene and close such institutions due to links with extremist organisations or their funding, and because extremist ideology was promoted there and young people were radicalised.

Around 800 children in the Muslim community should be attending school in Estonia, but nearly 20 per cent of them are educated at home or attend school in their country of origin. Attendance at Estonian schools supports integration and prepares young people for life in Estonian society and its cultural environment.

Islamic religious symbols and practices are becoming increasingly visible in the public space and may generate social tensions. In Estonia's cultural context, these symbols and customs may be unfamiliar and, in certain cases, may conflict with Estonian law.

Terrorist propaganda

For years, terrorist propaganda has been a global problem because it acts as a catalyst for radicalisation and facilitates terrorist crimes. Individuals from Europe who travelled to Syria and Iraq in the previous decade and joined ISIS – so-called foreign fighters – were recruited through terrorist propaganda.

In recent years, those who have planned and carried out terrorist attacks in Europe were born in Europe. They radicalised independently, without leaving their home countries, often under the influence of terrorist propaganda. They do not necessarily maintain an allegiance to a specific terrorist organisation. One of the main activities of terrorist organisations is to spread propaganda in order to attract new followers, supporters and perpetrators of attacks. Young people are particularly vulnerable and receptive to such messaging.

Social media and the dark web are used for radicalisation, recruitment, incitement to violence and to facilitate attacks.

Algorithms also contribute to the dissemination of terrorist content. Once a user engages with such material, algorithms increasingly steer similar content towards them.

Supporters of ISIS ideology actively participate in groups that bring together young Muslims. Within these groups, young people experiencing an identity crisis are singled out and then guided into closed groups that contain more radical content. The main platforms used are Telegram, TikTok, Session, Discord, Facebook and X.

ISIS recruiters are also active on gaming platforms, where young users are offered the possibility of transferring in-game experiences into real life. In these environments, users can play as terrorist characters, using associated symbols.

Radicalisation often occurs unnoticed, as signs of concern in young people's online communication can be difficult to identify in time. Mental health problems and social isolation increase vulnerability. In addition, terrorist organisations employ online recruiters who specialise in targeting young people. Terrorist propaganda increasingly consists of memes and short videos, with a strong focus on gaming platforms. The emphasis is on visually engaging content that resonates with young audiences.

Administrators of online channels that disseminate jihadist propaganda are often minors themselves and may be active in multiple groups at the same time. Radicalisation is typically based on Salafist principles, reinforced by other anti-Western narratives. Different extremist ideas merge into hybrid ideologies.

Since the beginning of the Covid-19 pandemic, the number of influential online religious figures has also increased. Instead of attending a specific congregation, individuals increasingly seek religious guidance online, where self-appointed religious figures may lack theological grounding and are more likely to promote radical views.

ISIS has tailored its propaganda to reach young audiences. To capture the attention of young people in Western countries, it uses, for example, Japanese-style comics and video game themes. Messages aimed at young people are framed in the language of online culture.

Yevgeni Andreyenok: from violent social media content to Islamist ideology

Yevgeni Andreyenok first came to the attention of Estonian law enforcement in 2021, when he was a minor and was found in possession of child sexual abuse material. At the same time, propaganda material from the ISIS terrorist organisation was found on his computer. He also showed an interest in fascism. According to his own account, he was drawn to violent online content.

Andreyenok was detained in May last year at Tallinn Airport to prevent him from travelling for terrorist purposes. According to the indictment issued by the Prosecutor's Office, he intended to travel via Turkey to Lebanon and then on to Syria in order to join ISIS, receive training for the commission of a terrorist crime and commit a terrorist crime. At the airport, he was carrying military equipment, military clothing and a medical kit.

In July 2025, Andreyenok carried out a life-threatening attack on a prison officer at Tallinn Prison, with the intent of committing an act against the Estonian state motivated by terrorist ideology. He has been charged with several terrorism-related crimes, including attempting to travel for terrorist purposes and committing a terrorist crime. Criminal proceedings against Yevgeni Andreyenok are ongoing.

Kremlin-backed right-wing extremism

In April 2025, at KAPO's proposal, the Police and Border Guard Board expelled Konstantin Gorlov from Estonia on the grounds that his activities posed a threat to the security of the Republic of Estonia and other Schengen member states.

There was no doubt in our assessment that in the event of Russian aggression, Gorlov would have acted in Russia's military interests.

Gorlov supported Russia's military and propaganda objectives and had contacts with individuals who acted in the interests of Russian intelligence services and the military. He sought to establish a unit in Estonia that could be used in Russia's military interests. Following the model of the Ratibor combat club linked to the Russian Imperial Legion, he founded Ratibor Estonia. The club's training sessions included practice in the use of bladed weapons and combat medicine.

Gorlov was connected to Andrei Votsygin, the leader of the Ratibor combat club in Perm, Russia. Members of that club have taken part in Russia's aggression, including operating a dedicated reconnaissance group in Ukraine. In addition to their training sessions, the club recruits participants for Russia's military aggression against Ukraine.

The Russian Imperial Legion is the paramilitary arm of the Russian Imperial Movement. Its fighters were active in Ukraine between 2014 and 2017 and later again in Bakhmut, where Russia committed war crimes. They have also operated in Syria, Libya and Central Africa.

The movement and the legion run a training centre called Partizan, where activists are trained by former Spetsnaz and FSB officers. All three organisations use media networks to disseminate messages, raise funds and promote activism, including on the battlefield.

The Russian Imperial Movement has been designated as a terrorist organisation under the United States and Canadian sanctions regimes as a Specially Designated Global Terrorist entity. The Russian Imperial Movement, the Russian Imperial Legion and their leaders are also listed under European Union sanctions.

PREVENTING AND COUNTERING INTERNATIONAL TERRORISM

Lone actors who are not formally linked to a specific terrorist organisation represent a growing threat.

The inadequate integration of immigrants increases the likelihood of radicalisation.

Events in distant regions such as the Middle East and the Sahel region of Africa can influence Estonia's security situation. Terrorist organisations operating in these areas may send fighters to Europe, where individuals who have received military training in conflict zones pose a threat.

Terrorist organisations may commission attacks in Europe through local supporters or hire criminals to carry out attacks for payment – a model described as "crime as a service". Through false flag operations, they seek to create safe havens. Afghanistan, the Sahel region and Somalia provide terrorist organisations with new fighters and generate fresh flows of foreign fighters to conflict zones. These regions also enable terrorist groups to increase their income, primarily by imposing various forms of taxation in areas under their control and by carrying out kidnappings for ransom.

Terrorism increasingly inspires autonomous networks of individuals who support terrorism because of their convictions but without direct instructions from terrorist organisations. Many gather in social networks where radicalisation takes place through the dissemination, promotion and consumption of violent material. Recruitment similarly occurs in online networks.

Migration and the terrorist threat

Estonia is a destination country for migration. More than half of those who arrive to study or work settle in Estonia on a long-term basis. Therefore, decisions to encourage or restrict migration directly influence the pace of growth of the Muslim community.

The low-skilled labour recruited in Estonia generally does not come from Europe. A significant share of short-term workers come from high-risk countries.

As terrorists may use both legal and illegal migration channels to reach Europe, it is essential to monitor migration flows and identify high-risk individuals before they arrive in Estonia.

The risks associated with short-term migration can generally be managed and depend largely on the capacity of authorities to carry out effective checks and procedures, as well as on the willingness and ability of countries of origin to cooperate. Law enforcement and security cooperation is often difficult with weak states and countries that maintain limited diplomatic relations with Estonia.

The effects of long-term migration are more complex to manage. A key factor is the willingness of immi-

grants to adapt and integrate and the state's ability to set and uphold clear requirements.

Integration is highly resource-intensive and presents a great challenge. Where integration is inadequate, frustration may increase the likelihood of radicalisation, making immigrants more vulnerable to recruitment by extremists or criminal networks.

As in 2024, when we identified a security risk in relation to a visiting imam, a foreign imam also stayed in Estonia briefly at the beginning of 2025 and posed a potential security concern due to the dissemination of antisemitic messages.

Criminals also use Estonia as a transit country. In previous years, several individuals linked to terrorism have travelled through Estonia en route to Russia or, conversely, from Russia to Europe. Beyond transit cases, we have observed that some delegations officially invited to Estonia by various institutions have included individuals who have publicly justified terrorist acts. For example, in 2025 a delegation visited Estonia that included at least one member who had previously, in public and verifiable statements, praised the terrorist organisation Hamas and the attacks it had carried out.

Key developments to monitor in Estonia:

Rising labour and education migration. The low-skilled labour recruited in Estonia generally does not come from Europe. A significant share of short-term workers come from high-risk countries.
Increased migration from countries where terrorist organisations operate or where conservative forms of Islam are widespread may increase the number of individuals in Estonia who have limited readiness to adapt and integrate.

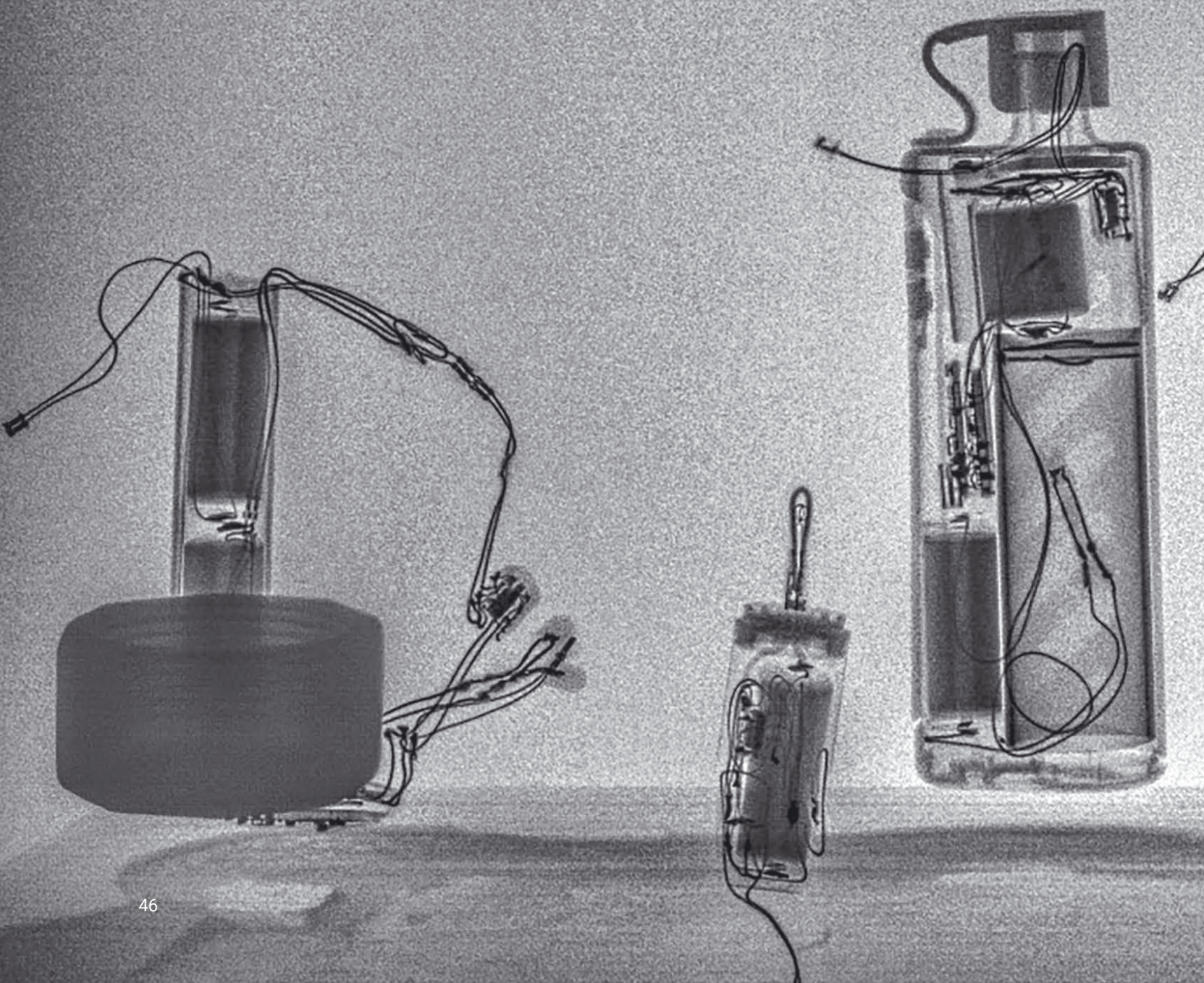
Escalating conflicts in the Middle East. For example, the conflict between Iran and Israel has led to attacks in Europe against Jewish communities and Israeli targets.

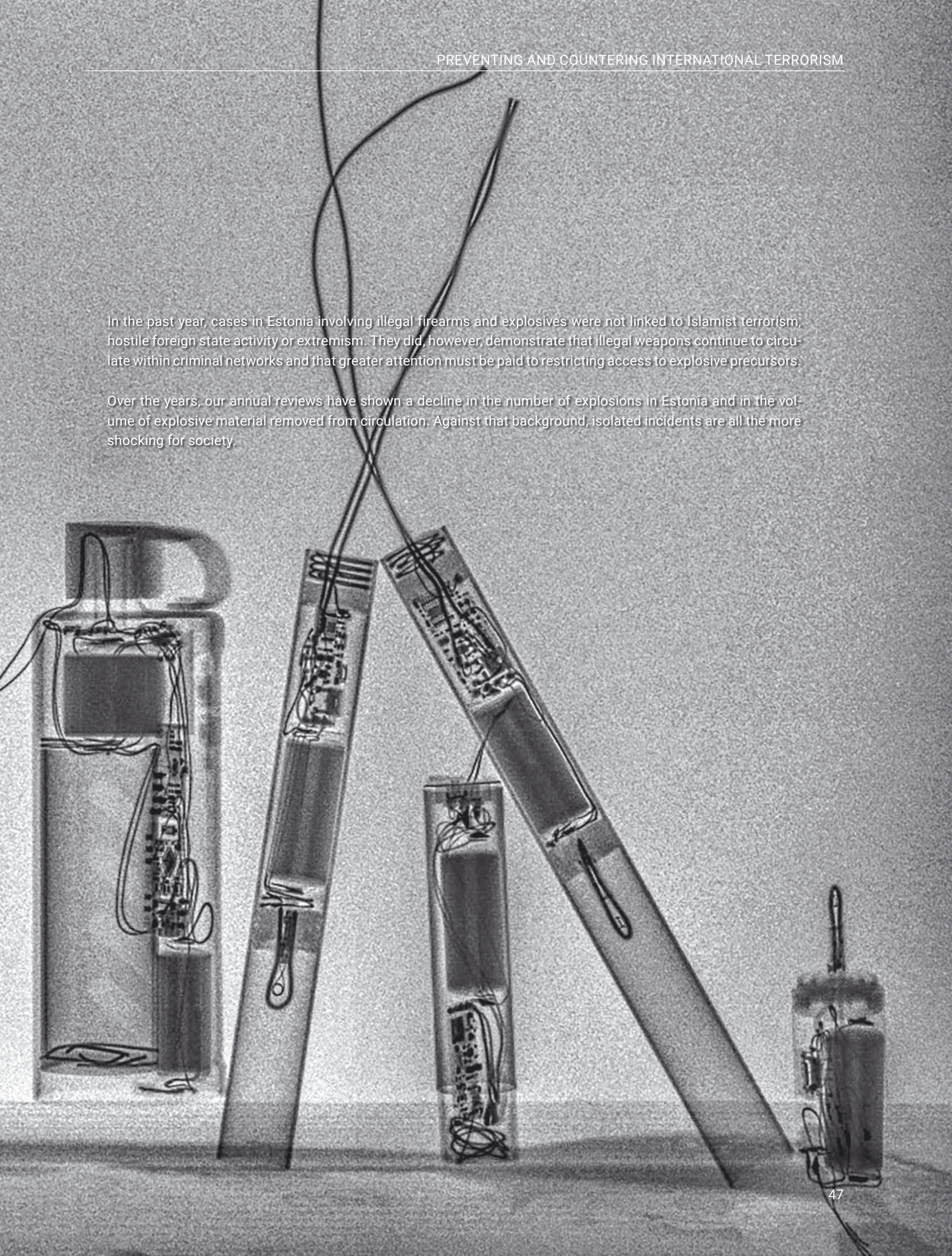
Independent online radicalisation. Radical networks operate on social media platforms, and recruitment efforts also take place on gaming platforms. Extremists target young people who seek a sense of belonging, lack self-confidence or struggle with mental health issues, with the aim of radicalising them and potentially using them to carry out attacks in Europe.

ILLEGAL HANDLING OF FIREARMS AND EXPLOSIVES

The threat to Estonia's security from illegal firearms and explosives has not increased. The risk would rise if Russia's full-scale war against Ukraine were to end or the conflict were frozen and weapons used in the war were to circulate through criminal networks.

In such a scenario, Estonia would likely become a transit country for arms trafficking. At present, there are no signs that weapons from the conflict zone have reached Europe.





In the past year, cases in Estonia involving illegal firearms and explosives were not linked to Islamist terrorism, hostile foreign state activity or extremism. They did, however, demonstrate that illegal weapons continue to circulate within criminal networks and that greater attention must be paid to restricting access to explosive precursors.

Over the years, our annual reviews have shown a decline in the number of explosions in Estonia and in the volume of explosive material removed from circulation. Against that background, isolated incidents are all the more shocking for society.

Explosion at a Tallinn shopping centre

On the weekend before Christmas, an explosion occurred at the Ülemiste shopping centre in Tallinn. A cleaning worker was emptying a bin next to a grocery store when an improvised explosive device detonated inside it. The victim required hospital treatment. Metal washers that had been placed inside the device to cause shrapnel injuries were removed from the victim's legs. In addition to open wounds, one washer caused a fracture of the victim's kneecap. Fortunately, the injuries were not life-threatening, and no other persons nearby were physically harmed.

People in the shopping centre were evacuated and investigators attended the scene. In cooperation with partner agencies and the shopping centre, investigators quickly identified a possible suspect, Artur Boiko, who has previously been convicted of several criminal offences. Boiko had earlier worked as a cleaner at the Ülemiste shopping centre but had been dismissed due to problems at work.

Investigative operations carried out at Boiko's residence are regarded by KAPO investigators as some of the most complex in its history in terms of ensuring safety. The four-day search was resource-intensive and time-consuming due to the risk of explosion. Nearly 8 kilograms of homemade triacetone triperoxide (TATP) and dozens of improvised devices of varying size resembling explosive devices were found at the suspect's home. On visual inspection, it was not immediately clear whether they contained explosives. Only detailed bomb disposal examinations at a testing site confirmed that some of the devices did not contain explosive material. The precise nature of the devices will be determined through further forensic analysis. Many of the devices were fitted with a mechanism capable of triggering an explosion and a compartment for explosive material, although the explosive substance itself had not been inserted.

During questioning, the suspect has provided investigators with explanations regarding the explosion at the Ülemiste shopping centre, his motives and the homemade explosives and devices found at his home. The ongoing pre-trial investigation will assess which of his statements are corroborated by other evidence. As the investigation is still underway, no further details can be disclosed at this stage.

More than 100 people took part in the investigative operations following the explosion at the Ülemiste shopping centre on 20 December 2025. In addition to KAPO officers, around 90 police officers, ten rescue personnel, six bomb disposal experts and a police dog were involved.

Source: Estonian Internal Security Service

Disrupting aviation may lead to criminal proceedings

Drones have disrupted operations at major European airports, prompting flight suspensions to ensure safety. While such suspensions cause economic loss and inconvenience to passengers, a collision between an aircraft and a drone or the dazzling of a pilot with a laser can have catastrophic consequences and cost dozens of lives. In Estonia, too, aircraft and helicopters are interfered with out of misguided curiosity, ignorance or simply boredom.

Such incidents generally fall into two categories. The most common involves flying drones in or near airport areas and along take-off and landing corridors. A remote pilot who ignores drone regulations may face serious consequences, including confiscation of the drone and criminal proceedings.

Targeting aircraft with lasers can, according to aviation safety authorities, damage a pilot's eyesight and cause temporary blindness, potentially resulting in an air accident. This is particularly dangerous during take-off and landing. KAPO receives reports of such incidents every month.

In several cases, those identified as using lasers have been minors who became involved out of boredom and ignorance.

Under the Estonian Penal Code, disrupting aviation – that is, creating a risk of an aviation incident – may qualify as an offence against aviation safety even if no accident occurs. The offence is punishable by a fine or by up to 10 years' imprisonment. The prospect of criminal proceedings often comes as a surprise to drone operators or laser users. We therefore reiterate that interfering with aircraft can have severe consequences and is punishable by law. Drones and lasers should be used only in accordance with regulations and kept well away from aircraft.

In 2026, Harju County Court convicted an individual who had intentionally and repeatedly aimed a laser sight at a helicopter. The court imposed a sentence of three years and two months' imprisonment for endangering flight safety, creating a risk of an aviation incident and unlawfully using a firearm laser sight.

The sentence will not be executed provided that the individual does not commit another intentional criminal offence during a probation period of three years and three months.

Drones

Russia's war of aggression against Ukraine has ushered in the era of drones. As long as our neighbouring country continues its military campaign, we must assume that the drones that fell on Estonian territory in 2025 will not be the last. At 4:45 a.m. on 24 August 2025, an FP1 drone entered Estonian airspace from Latvia and flew in a straight line until it crashed in a field in the village of Aakre in Tartu County. Forensic analysis identified traces of explosives typically used in attack drones. This type of drone can carry between 60 and 120 kilograms of explosives over long distances. The exact quantity carried by this drone cannot be determined, as the explosive detonated completely on impact.

The drone's arrival in Estonia coincided with a Ukrainian drone strike on the Novatek terminal at the port of Ust-Luga in Russia's Leningrad region, approximately 50 kilometres from the Estonian border.

As there is currently no legal cooperation with Russia, it is not possible to determine the drone's flight path before it entered Latvian airspace or where it began its journey. The investigation found no indication that the drone was deliberately directed towards Estonian territory or that Estonia was the intended target.

KAPO and the Estonian Prosecutor's Office have closed the criminal investigation, as all feasible investigative steps to identify a responsible party have been completed. Should new information emerge, the investigation will be reopened.

On the early morning of 27 September 2025, the nose section of a Gerbera drone of Russian origin was found on a beach in Häädemeeste rural municipality in Pärnu County. The fragment, a piece of foam with visible fracture marks, lay five metres from the waterline among reeds. It posed no threat to life or health and had drifted ashore onto the Pärnu coastal meadow from the sea.

On the night of 24 March 2026, when Ukraine struck the port of Ust-Luga, located 35 kilometres from the Estonian border, a Ukrainian drone that had strayed off course crossed the Narva River into Estonian airspace and struck the chimney of the Auvere power plant. No one was injured in the incident.

If you find a suspicious drone:

- **Do not approach the drone.**
- **Immediately call the emergency number 112.**
- **Move to a safe distance.**
- **Warn people nearby and do not allow anyone to approach the object.**
- **Do not share its location on social media.**

Source: Estonian Rescue Board

ECONOMIC SECURITY

The loyalty dilemma of individuals with dual citizenship poses both corruption and security risks.

Sanctions constrain Russia's aggression. Companies that provide support services enabling the movement of sanctioned goods contribute to the continuation of that aggression.

Crypto-asset services that are not subject to traditional banking rules lead to security risks.

In safeguarding economic security, KAPO works to prevent foreign economic pressure that could undermine Estonia's national security or threaten its sovereignty through economic means.

The highest security risks in economic activity are associated, in particular, with critical infrastructure sectors: energy, information technology, transport and the defence industry.

Hostile actors collect publicly available online information about providers of essential services, the functioning of critical infrastructure and the individuals associated with these sectors, and also conduct on-site observations. We encourage those working in critical infrastructure to carefully consider the potential consequences before sharing sensitive information or details about their colleagues and their roles.

KAPO also monitors foreign investment, international sanctions and the provision of essential services. Both Russia and China seek to identify and exploit Estonia's vulnerabilities.

Sanctions are effective

Sanctions are intended to weaken the Russian Federation's war machine and its ability to sustain aggression in Ukraine. Accordingly, they cover a broad spectrum, ranging from prohibited goods to services and financial flows. International sanctions have demonstrated their effectiveness, but their consistent enforcement remains essential.

Strict sanctions on strategic goods have forced Russia to build complex and costly procurement networks to obtain the equipment and technologies it needs. To conceal the true end use of goods from manufacturers, who are required to verify lawful end users, and from investigative authorities, numerous shell companies are established, intermediaries engaged, and convoluted payment schemes and transport routes employed.

In Estonia's case, the main concern lies in the misuse of the country's favourable geographic location, previous business ties with Russia and abuses of the

country's open economic environment to facilitate sanctions circumvention – for example, by ordering goods in the name of companies registered in Estonia but not actually operating. Estonia's good reputation is exploited by ordering goods through Estonian companies and then diverting them to Russia through unlawful channels or third countries.

A breach of goods-related sanctions does not require a direct export from the European Union to Russia; it is equally prohibited to supply sanctioned goods to Russia via third countries.

Nearly one-third of goods declared as transiting Russia do not reach their stated final destination. In light of this loophole in the sanctions regime, Estonia has proposed to European Union institutions that a general transit ban be imposed on goods that are prohibited from export to Russia but are declared as bound for third countries and transported via Russian territory.

Estonia can prohibit land transit through Russia by applying a national sanction, which does not require European Union consensus. However, if Estonia were to close its border unilaterally, goods would be redirected to Russia through another country. Steps have already been taken to enable Russia's neighbouring states – Finland, the Baltic states and Poland – to coordinate national sanctions in the future and, if necessary, jointly prohibit land transit through Russia. This would further restrict the Kremlin's access to sanctioned goods. Sanctions remain the most effective non-military means of constraining Russia's aggression. In the near future, international sanctions imposed on Russia are neither expected to be lifted nor eased.

Since April 2025, the Estonian Tax and Customs Board has been responsible for investigating violations of cash and goods-related sanctions. KAPO continues to investigate violations of service and financial sanctions, the unlawful transport of prohibited strategic goods, and the cross-border movement of military weapons and military-grade ammunition.

Estonian logistics companies operating in Central Asia must exercise particular caution. Currency transfers in euros or dollars to accounts held with Central Asian banks may subsequently be forwarded to sanctioned entities in Russia or to companies registered in the region that are linked to sanctioned individuals or entities. In such cases, there is a risk of breaching financial sanctions.

Strategic goods for Russia's defence industry

Since the start of the full-scale war, Russia has intensified its efforts to acquire goods produced in Western countries, and its defence industry remains dependent on Western products. Weapons and components recovered from battlefields in Ukraine show that military goods, dual-use items and civilian products used in the defence sector continue to reach Russia from Europe and the United States. Russia's objectives are also supported by strategic partners in other countries – foremost among them China, which supplies Russia's defence industry with both domestically produced goods and items purchased from Western countries.

Several companies operating in Estonia procure goods from Western countries to fulfil orders placed by Russia's defence industry. The management boards of such companies often include citizens of the Russian Federation or e-residents who have no genuine ties to Estonia. There have also been cases in which company employees were physically located in Russia and placed orders from there, using an Estonian-registered entity to mislead Western suppliers.

Estonian companies' business activities in Russia

Because of the war, many Estonian companies have ended their business activities in Russia or are seeking to exit the market, as the current regime imposes restrictive measures on them. Some entrepreneurs have lost all control over the assets and operations of their subsidiaries and affiliated companies. At the same time, certain Estonian companies have not severed their business ties and continue to maintain previously established corporate entities in Russia. These subsidiaries and affiliated companies, registered in Russia, mainly operate in wholesale trade, transport and logistics and must exercise particular diligence in complying with continually expanding sanctions.

Order from the Russian Ministry of Defence

We have identified Estonian citizens, individuals residing in Estonia under residence permits and companies registered here that knowingly procure goods for Russia.

In 2025, a court convicted Daniil Haitin of violating international sanctions, illegally transporting strategic goods, forging documents and using forged documents. The court also convicted Haitin's company, Marine Technics Baltia OÜ, of violating international sanctions and illegally transporting strategic goods. Haitin received a suspended sentence of 4 years and 11 months. His company was ordered to pay 160,000 euros to the state as a financial penalty.

Marine Technics Baltia had previously sold equipment that was later supplied to Rybinskaya Verf, a company that fulfilled orders for the Russian Ministry of Defence. The shipyard manufactures BK-16 and BK-10 military patrol boats equipped with automatic weapons. Marine Technics Baltia sold the yard thermal imaging cameras, waterjet propulsion systems and marine engines, all of which qualify as military goods.

The equipment was exported from Estonia, Italy, and Germany to Russia and would have required a special export licence, which neither Haitin nor his associated company possessed.

In a similar case, Andrei Shevlyakov was already acting in Russia's interests before the start of the full-scale war in Ukraine. He systematically purchased Western electronic components from Europe and the

- In 2015, Marine Technics Baltia OÜ signed a contract with the Russian company LLC MT-Group.
- In April 2022, Haitin agreed with his Russian partner on the sale of a gas generator unit for 87,000 euros.
- On 4 May 2022, officials of the Estonian Tax and Customs Board seized the unit at the Narva border crossing on suspicion of a breach of sanctions.
- Through the Hungarian company Antey Power Kft, four gas generator units worth 336,200 euros were exported. In June 2022, the shipment was intercepted in Pärnu County at the Uulu car park before it reached the Ikla border crossing. The declared end destination was the Russian company OOO Zavod PSM.
- These units could have contributed to strengthening Russia's military and technological capabilities.
- In 2021, Haitin placed an order with the Finnish company Elektro-Arola OY for the purchase of radio transmitters on behalf of the Estonian company Dandelion Teeninduse OÜ.
- In 2022, the New Zealand manufacturer of the radio transmitters requested that Haitin provide an end-user certificate confirming that the devices would not be supplied to a sanctioned end user.
- Haitin submitted a forged document bearing the name and signature of an employee of the Estonian Rescue Board in an attempt to conceal the true end user of the devices in Russia.

United States and smuggled them to Russia. Many of the components he ordered were classified as dual-use goods and, even before the full-scale invasion, required an export licence from the Strategic Goods Commission under the Estonian Ministry of Foreign Affairs. Shevlyakov did not hold such a licence.

Since the start of Russia's full-scale war against Ukraine, the export of dual-use goods to Russia has been prohibited.

In 2025, Shevlyakov was extradited from Estonia to the United States for trial.

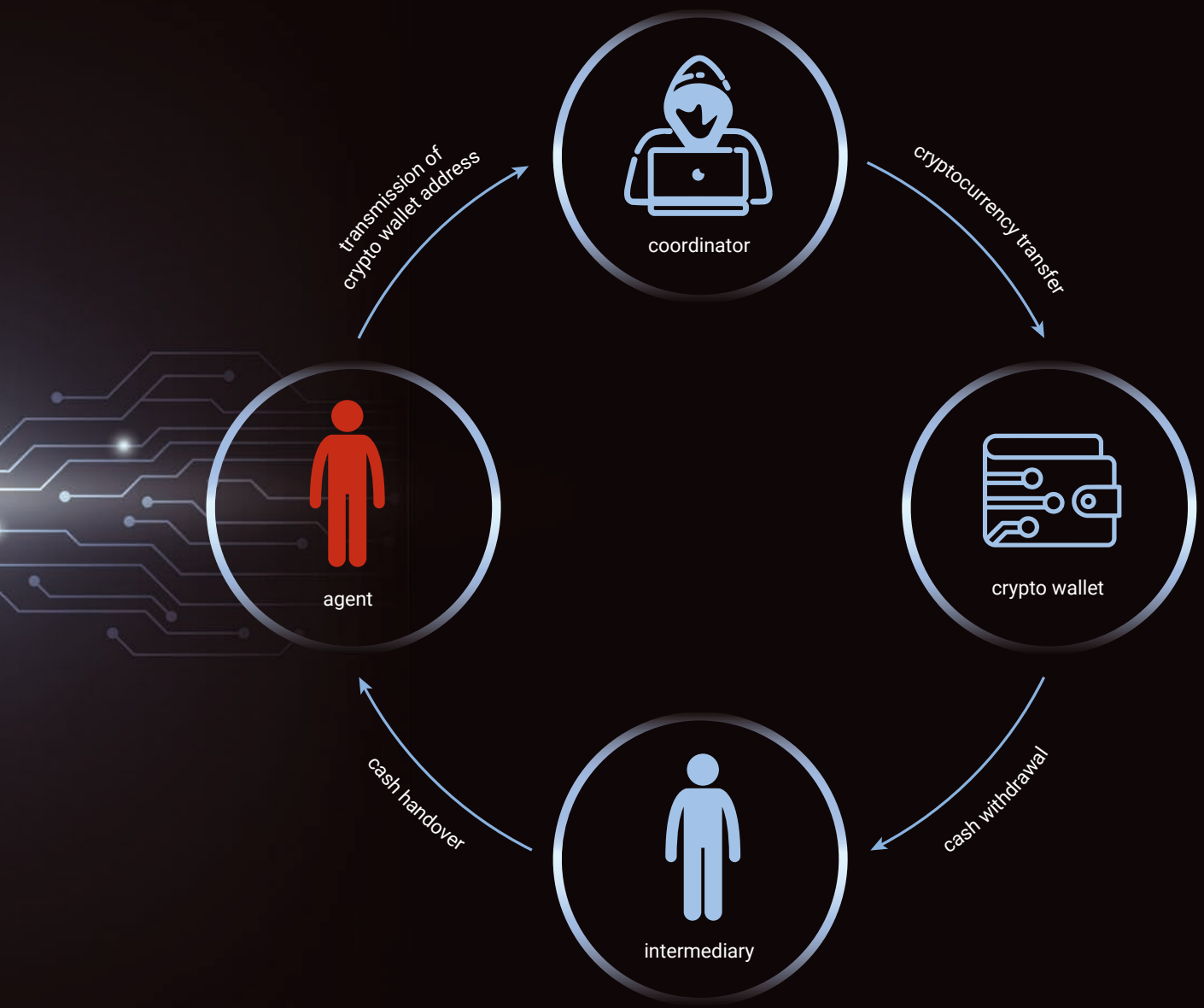
Successive sanctions packages and regularly updated lists of strategic goods have made it more difficult – though not impossible – for Russia's defence industry to procure components. Russia continues to exploit manufacturers' limited scrutiny of their customers and weaknesses in the European Union's external border customs procedures. In cooperation with the Tax and Customs Board, the Strategic Goods Commission and the Financial Intelligence Unit, we are working to prevent Russia's defence industry from using Estonia as a procurement route and to block such acquisitions from Europe.

SECURITY RISKS RELATED TO CRYPTO-ASSETS

Crypto-assets are not subject to the same requirements as traditional banking. Crypto transactions can offer anonymity to the parties involved and, in some cases, provide a means to circumvent international sanctions. Virtual currencies are not used solely to finance terrorism – they may also be used to fund influence and intelligence activities, such as paying agent fees in cryptocurrency.

PAYMENT TO AN AGENT IN CRYPTOCURRENCY

An agent recruited by a Russian intelligence service sends the address of a cryptocurrency wallet belonging to an intermediary. The agent's coordinator transfers funds to that wallet. The intermediary withdraws the transferred amount in cash. The agent is informed of the time and place where the cash will be handed over.



ANTI-CORRUPTION EFFORTS

Corruption undermines public trust in the state, erodes democratic values and distorts fair competition, thereby constraining economic development. The risks associated with corruption that threaten national security primarily involve senior officials and large-scale investments in the defence, energy and other strategic sectors.

In ensuring corruption-free governance and the equal treatment of interest groups, attention must also be paid to the role of think tanks alongside more visible areas of corruption risk. The activities of existing and emerging think tanks require transparency. While political party financing is subject to oversight and policymakers are required to declare their interests, no comparable rules apply to think tanks that seek to influence political decisions or to their members.

Transparency in the funding of think tanks and the studies they conduct would help mitigate corruption risks. It is equally important that meetings between think-tank representatives and senior officials be recorded in the lobbying register to ensure transparency in political decision-making. A lack of transparency creates opportunities for improper arrangements with high-level officials.

The findings and opinions produced by think tanks must be impartial and free from external influence, meaning they must not depend on funders. Only in this way can Estonia ensure that political decisions are not shaped by narrow interest groups or financing from third countries.

Revolving-door effect

In the defence and energy sectors, corruption risks stem from the scale of investments and the pressure to make rapid decisions. Developing Estonia's defence industry and strengthening energy independence are critical objectives, but financial decisions must be made in accordance with the principles of impartiality and equal treatment. Given the magnitude of these investments, consistent auditing and stronger oversight mechanisms are required. One approach is the use of so-called red teams to identify vulnerabilities in procurement processes, including in areas classified for national security reasons.

Because of Estonia's small size, decision-makers and business representatives may have close ties. Therefore, officials involved in public procurements worth hundreds of millions of euros should be subject to a cooling-off period upon leaving office. This would help prevent conflicts of interest in which information, networks or influence acquired in a previous role affects decisions in a subsequent position. In recent years, a revolving-door effect – the movement of senior officials into private-sector roles in the same field they previously regulated or oversaw – has become evident in senior positions related to national defence. To uphold the principles of fair and equal use of public funds, situations must be avoided in which entrepreneurs seek state support for defence-related product development from former colleagues.

Procedural restriction on transactions with connected persons

The purpose of Estonia's Anti-Corruption Act is to ensure that public duties are performed impartially and with integrity. If a person decides on a transaction from which they may personally benefit, it is not possible to be certain that the decision was made correctly and treated all parties equally. Even if the person regards themselves as impartial, a reasonable suspicion of bias remains. Justice requires not only a substantively fair outcome but also a process that is visibly fair and open to scrutiny.

The core principle is widely recognised internationally: a person who has a personal or private interest, or any other relevant connection in a matter under consideration, should not participate in deciding that matter.

Using powers entrusted for the performance of public duties in pursuit of private interests undermines the impartiality of public authority and erodes society's trust in the integrity of the state, local governments and other public institutions, as well as in the reliability of official decision-making and, ultimately, in the lawfulness of public decisions. When free competition no longer operates effectively and persons connected to an official are favoured in the exercise of public authority, other market participants may be tempted to secure preferential access through improper means. More broadly, confidence in the ability to operate lawfully in the country begins to erode. As noted in our previous annual review, this constitutes a threat to national security.

The drive to relax anti-corruption rules is first reflected in allowing a greater scope for private interests in the exercise of public authority. Until now, the buying and selling of official decisions or acts has been punishable under Estonian law as the criminal offence of giving or accepting a bribe. In situations involving a conflict between private and public interests, making a decision or performing an act with a monetary value of 40,000 euros or more on a large scale has been punishable as the criminal offence of violating a procedural restriction.

According to a draft amendment currently under consideration, only a knowing breach of a procedural restriction laid down in the Anti-Corruption Act that causes substantial damage or results in substantial financial gain for the official or a connected person would constitute a criminal offence. In other words, the legislative intent is to make punishable not the creation of a corruption risk involving a large monetary value, but only the realisation of that risk in the form of damage of 40,000 euros or more or substantial financial gain. Such a narrowing of the criminal law provision would reduce the scope of criminal liability for corrupt acts committed by officials. Unlike "substantial damage" or "large scale", the term "substantial gain" has not previously been defined in Estonian criminal law.

On 15 March 2007, the Estonian legislature defined the large-scale violation of a procedural restriction as a criminal offence harming the duty of integrity of a public official. At that time, the offence of large-scale violation of a procedural restriction was introduced to replace the previously applicable general offence of abuse of office.

Importing corruption from Russia

In south-eastern Estonia, a security risk arises from local companies employing workers who reside in Russia and hold dual Estonian–Russian citizenship. Given the wage differences between Estonia and Russia's Pskov region, it is understandable that recruiting workers from across the border may appear financially attractive to Estonian employers. However, alongside reduced labour costs, the use of workers from Russia carries risks that can far outweigh any savings if they materialise.

Russian residents who regularly cross the border to work in Estonia bring with them counter-intelligence risks and exposure to corrupt practices.

Individuals who frequently cross the border are repeatedly exposed to Russian intelligence and security officers. These officers systematically profile travellers, assess their suitability for covert cooperation, recruit them for activities hostile to Estonia and subsequently manage them as agents. There is, however, one critical difference: if such an agent is arrested and prosecuted in Estonia, the handler and the service that recruited them will simply abandon the individual who cooperated.

Corruption as a security risk

Russian nationals employed in Estonia may engage in bribery, a practice not seen in Estonia for years. Since 2025, in cooperation with the Estonian Prosecutor's Office, we have drawn attention to a problem at the Koidula road border crossing, where administrators of the waiting area accepted bribes.

In October 2025, Tartu County Court convicted three employees of the Koidula border crossing waiting area – Liivi Chizhova, Valentina Semyonova and Yelena Ivanova – of accepting bribes. All three hold dual Russian and Estonian citizenship. They reside in Russia but commuted to work in Estonia. The women agreed among themselves to abuse their positions by offering priority access to the border crossing in exchange for payment. The agreed price for one crossing was 50 euros, though higher sums were accepted when offered. Clients provided the truck registration numbers and booking numbers assigned to their vehicles, and priority passage was arranged. Payments were made in cash or by bank transfer. In this way, dual citizens residing in Russia imported a pattern of corrupt conduct common in Russia into Estonia, where such behaviour is unacceptable.

One client, Vyacheslav Yefimov, who paid bribes and was also a security guard at the border checkpoint waiting area, used Chizhova's services at least on three occasions to obtain priority passage. In January 2026, he was convicted of activities against the security of the Republic of Estonia, specifically acting in the interests of, or on behalf of, a Russian intelligence service and of collecting and transmitting information. In the autumn of 2022, at the proposal of FSB officer Nikolai Tarasov, Yefimov entered into covert cooperation with the FSB Border Service. Tarasov and Yefimov signed an agreement, which Yefimov signed in his own hand. They met at Yefimov's home in Pechory and also communicated through messaging applications.

Yefimov provided the FSB with information about staff at the Koidula waiting area, individuals associated with Estonian state authorities who crossed the Estonian–Russian border, the movement of drones and military equipment at the Koidula border crossing and details about border guards, construction machinery operating near the crossing, interviews conducted at the checkpoint, specific officers, cable installation works carried out from the Koidula railway line to the border crossing, and a company performing electrical work near Koidula railway station and its vehicles.

Tartu County Court sentences:

Valentina Semyonova

Three years and six months of imprisonment, with four months to be served immediately. The state confiscated assets totalling 19,077 euros.

Yelena Ivanova

Two years and eight months of imprisonment, with four months to be served immediately. The state confiscated assets totalling 8,993 euros.

Liivi Chizhova

Three years and two months of imprisonment, with four months to be served immediately. The state confiscated assets totalling 5,154 euros.

Risks for employers

According to our information, a significant share of the workforce employed by Estonian essential service providers with a large Russian-speaking staff continues to reside in Russia. The Russian Federation's aggressive policy – including the use of force to assert territorial claims, such as in the Saatse Boot and at the Vasknarva river pier in Estonia – as well as other potential cross-border actions, such as the deliberate creation of a situation involving mass irregular migration, illustrate the volatility of border security. Employers who rely on workers residing in Russia make themselves dependent on the state of security relations between Estonia and Russia. If border crossing points are suddenly closed at the initiative of either state, companies may instantly lose part of their workforce and be forced to switch to local labour. For providers of essential services, this risk extends beyond the loss of employees to the leakage of internal information and a deterioration in service continuity and availability.

SECURITY IMPLICATIONS OF RUSSIA'S WAR OF AGGRESSION

Individuals who have taken part in Russia's war of aggression are being barred from entering Europe in order to mitigate the criminal and security risks they pose.

Russia's war of aggression against Ukraine has now entered its fifth year. There is still no end in sight, despite ongoing peace negotiations. Even if a ceasefire were agreed upon, its sustainability could not be taken for granted.

Estonia can help restrain Russia's aggression indirectly by collaborating with other European countries. This is achieved through sanctions and various other restrictions imposed on Russia by Western nations. These measures have a clear impact and must be maintained and strengthened.

In addition to the open warfare in Ukraine, Russia and its intelligence services have waged a covert campaign against Europe. This campaign includes sabotage, cyber-attacks and targeted attacks against individuals, along with other types of hostile activities collectively referred to as hybrid warfare. Unlike the visible consequences of traditional warfare, the effects of hybrid warfare are often hidden from public view. The tactics used are designed to obscure the involvement of Russia and its intelligence services.

Hybrid attacks typically rely on individuals recruited through social media, many of whom have criminal backgrounds. The primary motive for committing these offences is financial gain, even though the compensation offered by those commissioning these attacks tends to be modest. During the war against Ukraine, Russian intelligence has developed infrastructure, recruited personnel and established chains of command to conduct operations against Europe. Given the methods and patterns of behaviour of Russia's intelligence services, there is little reason to assume that Russian attacks against Europe will stop once the war in Ukraine ends, or that the infrastructure will simply be dismantled and recruited individuals disbanded. Russia's activities aimed at Europe will likely continue for as long as it seeks to assert its interests in the region. Therefore, KAPO and other European security agencies are expected to face challenging years ahead.

Prevention is always easier and less costly than dealing with the consequences. A common feature among those who carry out attacks against Europe is their access to European territory. They are either permanently present in Europe or have entered on visas. Estonia has revoked the residence permits of several individuals on security grounds and returned them to Russia. The European Union has further restricted the issuance of visas to Russian citizens, including by ending the issuance of long-term visas. However, these measures are still insufficient.

One likely recruitment pool for future attacks against Europe consists of individuals who have fought on Russia's side in the war of aggression against Ukraine – Russian combatants. These individuals participate in aggression and pursue the criminal objectives of the Putin regime as members of the Russian armed

forces and other armed formations. Many of these individuals are experienced in the use of violence, with nearly 200,000 offenders having been sent from Russian prisons to the front lines. A significant number have taken part in war crimes and crimes against humanity while fighting in Ukraine. Most of these combatants have been ideologically indoctrinated against the West and are primarily motivated by financial gain. This background makes them appealing recruitment material for both Russian intelligence services and criminal groups engaged in operations against Europe.

To enhance the security of Estonia and the Schengen area as a whole, and to prevent combatants from travelling to Europe in the future, we have initiated the process of adding Russian combatants to the Schengen entry ban list. We will continue this initiative and, in cooperation with Estonia's interior and foreign ministries, other government agencies and like-minded European countries, will work to ensure that more European states join this effort. In parallel, Estonia is working towards a long-term European Union-wide solution to address the risks posed by combatants. Russian combatants will have no place in Europe in the future.

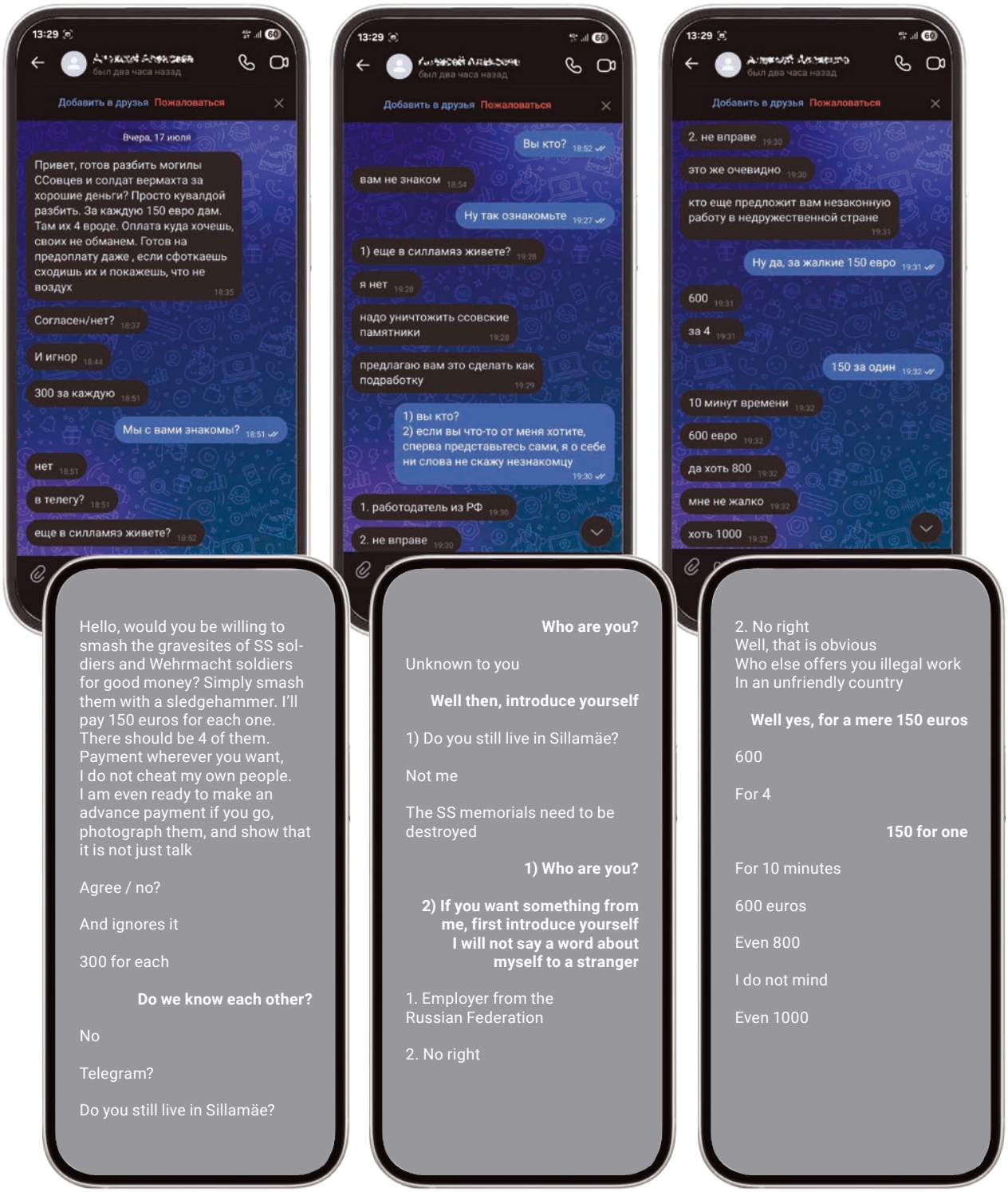
In September 2025, Ihor woke up in his home. He ate breakfast, checked the news and the internet, and set off for Moscow. From there, he travelled to Belarus, then to Poland, and finally reached his destination – Estonia – by bus.

Ihor was born and raised in Donetsk. He obtained a master's degree from Donetsk National Technical University, which now also trains reservists destined for the Russian Air Force. Ihor has spent most of his life in Ukrainian territory occupied by Russia.

In February 2022, just four days before the start of Russia's full-scale aggression against Ukraine, Ihor was mobilised into the armed forces of the so-called Donetsk People's Republic, which in practice form part of the Russian armed forces.

He was assigned to military unit S/O 08826, which is actively engaged in the war against Ukraine, and trained as a sniper. The unit took part in the battles of Avdiivka, Marinka and Krasnohorivka and played a significant role in the destruction of those cities. Ihor was discharged from military service on health grounds.

In 2025, he arrived in Estonia and applied for temporary protection. At KAPO's proposal, the Estonian Police and Border Guard Board refused to grant it and expelled him from the country. As criminal proceedings had been initiated against him in Ukraine on charges of treason, he was handed over to the Ukrainian authorities.



Hello, would you be willing to smash the gravesites of SS soldiers and Wehrmacht soldiers for good money? Simply smash them with a sledgehammer. I'll pay 150 euros for each one. There should be 4 of them. Payment wherever you want, I do not cheat my own people. I am even ready to make an advance payment if you go, photograph them, and show that it is not just talk

Agree / no?

And ignores it

300 for each

Do we know each other?

No

Telegram?

Do you still live in Sillamäe?

Who are you?

Unknown to you

Well then, introduce yourself

1) Do you still live in Sillamäe?

Not me

The SS memorials need to be destroyed

1) Who are you?

2) If you want something from me, first introduce yourself I will not say a word about myself to a stranger

1. Employer from the Russian Federation

2. No right

2. No right
Well, that is obvious
Who else offers you illegal work
In an unfriendly country

Well yes, for a mere 150 euros

600

For 4

150 for one

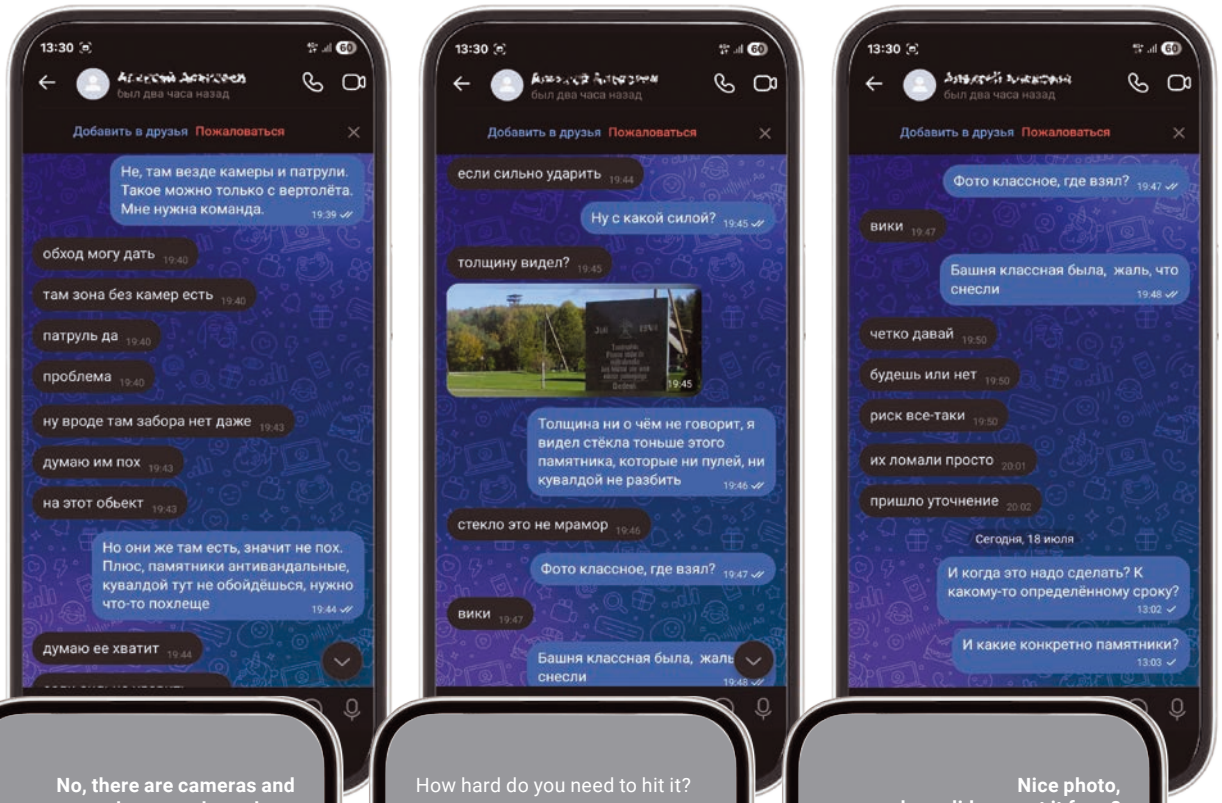
For 10 minutes

600 euros

Even 800

I do not mind

Even 1000



No, there are cameras and patrols everywhere there It can only be done from a helicopter. I need a team

I can guide you along a side route.

It is under camera surveillance

There is indeed a patrol
A problem

But it does not even seem as if there are fences there

I think they do not care
About that object

They are there, yes, which means they do care. Plus, the memorials are vandal-proof, A sledgehammer is not enough, something more powerful is needed

I think it is enough

How hard do you need to hit it?

Well, with what force?

Did you see the thickness?

Thickness means nothing, I have seen glass thinner than that memorial. Which cannot be broken either by bullets or with a sledgehammer

Glass is not marble

Nice photo, where did you get it from?

Wiki

It was a nice tower, shame it was torn down

Nice photo, where did you get it from?

Wiki

It was a nice tower, shame it was torn down

Say it plainly

Will you do it or not

There is a risk involved

They were simply smashed

A clarification has come

And when should this be done? By some specific date?

And which specific memorials?

Compiled by:
Marta Tuul

Edited by:
Margus Elings (Refiner)

Translation:
Margus Elings, Scott Abel (Refiner)

Design:
Ain Kaldra, Andre Poolma (Iconprint)

Photographs:
Delfi Meedia, Estonian Defence Forces, Estonian Internal Security Service, Estonian Police and Border Guard Board, Facebook, Iconprint, Ilmar Saabas, Shutterstock, Telegram, Tiit Blaat, VK, Weixin, YouTube

Layout, print:
Iconprint OÜ

(print)
ISSN 2228-1789

(web)
ISSN 2228-1797