Estonian Internal Security Service

Annual Review 2024·2025

Contents


Kaitsepolitsei

Dear reader,

This year, the Estonian Internal Security Service (KAPO) marks its 105th anniversary. Like the Republic of Estonia itself, KAPO has navigated significant shifts over the years. There have been times when it existed merely in name, serving as a symbol of the enduring value of freedom. Despite the challenges, the principal threat to Estonia's internal security has remained consistent: Russia.

Regardless of its public rhetoric, Russia is actively working to dismantle Europe's security architecture and carve out a privileged sphere of influence where NATO would be forced to withdraw. Russia considers Estonia to be part of this desired sphere of influence. Russia's brutal war of aggression against Ukraine has now entered its fourth year. In addition to Russia's visible military presence in Ukraine, a covert aspect of its armed forces operates throughout Europe.

In 2024, a series of arson attacks, vandalism, sabotage and attempted sabotage were carried out across Europe, all under the guidance of Russia's military intelligence service, the GRU. Through these hybrid operations, Russia aims to destabilise Europe and weaken the collective resolve to support Ukraine. However, Russia has miscalculated – such attacks do not undermine Europe but instead reinforce Western unity and resolve to continue support for Ukraine.

Hybrid warfare represents the initial phase of any military attack. KAPO works to anticipate and prevent non-military threats to safeguard the state against any potential military threats arising.

The future security landscape will be shaped by developments in Ukraine, particularly regarding whether peace is achieved and the conditions surrounding it. One certainty is that any peace agreement in Ukraine will not diminish the threats to Estonia's internal security. Once Russia can redirect its resources, it is likely to focus on other hostile activities. Potential threats include the illegal flow of weapons into Europe, which could end up in the hands of criminals or extremists. Additionally, Russian combatants returning from the front lines may also seek new "missions" in extremist organisations or criminal networks.

Russia's intelligence interest in Estonia remains consistent. In 2024, five individuals associated with the GRU were brought to court. Since the start of Russia's full-scale war in Ukraine, Estonia has revoked 15 residence permits for national security reasons, based on recommendations from KAPO.

In 2023, approximately ten individuals were arrested in connection with acts of vandalism against monuments and vehicles carried out under orders from Russia; they were convicted in 2024. Last year, the threat of similar attacks remained high. One such incident, instigated by Russia, occurred in Tartu, where a vehicle with Ukrainian licence plates was set on fire.

The Kremlin's support base in Estonia, primarily consisting of older residents, is in decline. As a result, Russia is shifting its influence operations towards younger Russian-speaking Estonians. It is essential that we protect these young people from being swayed by Russian propaganda.

As Kremlin-controlled media faces increasing restrictions, Russian propaganda efforts have shifted to social media. We are observing a rise in deepfakes and manipulations driven by artificial intelligence and algorithms. Social media shapes people's perceptions of the world and determines the information bubbles into which users are funnelled. As a result, users can become trapped in echo chambers or disinformation loops, with increasingly limited ability to verify what they see. Critical thinking remains the only reliable antidote to this issue. The Estonian education system rightly prioritises the teaching of critical thinking and media literacy.

Violent extremism seeks to attract young people online, transcending national borders and age groups. Lonely individuals who have faced difficult childhoods and seek a sense of belonging may find their way to extremist ideology when offered a compelling message. These messages often spread across multiple platforms and are quickly translated into many languages. For terrorist organisations, as well as for the Kremlin, disseminating propaganda is equally important as conducting attacks.

Recent amendments to Estonia's Information Society Services Act enable more decisive intervention against harmful content. However, we must also develop a comprehensive action plan to prevent radicalisation. The government must closely monitor hostile influence operations and violent extremist propaganda on social media. Although the threat of terrorism in Estonia remains low, even one attack would be unacceptable.

Virtual currencies are being used more frequently, not just for legitimate investments but as a key payment method in criminal activities. These activities include financing terrorism, carrying out hostile intelligence operations, conducting cyberattacks involving ransom demands, and engaging in organised crime. Innovation and digital payment technologies present new challenges for Estonia's law enforcement agen-

cies and its financial sector. Key issues include the need for legislative updates, increased risk awareness among service providers, effective implementation of due diligence measures and consistent efforts from law enforcement. As technology advances and cyber threats become more complex, cyber security is playing an increasingly vital role.

Today's security environment presents growing challenges and higher demands for KAPO, which is responsible for monitoring and preventing threats before they can harm Estonian society.

Raising awareness is crucial for effective prevention. In 2024, KAPO conducted numerous security training sessions and briefings, reaching nearly 2,000 officials and employees across various sectors. A strong collective front is essential – one that unites all Estonian residents, national security agencies, and partners both at home and abroad.

Much of KAPO's work as a security agency is hidden from adversaries and the general public. However, our activities remain fully transparent to the relevant oversight bodies, including the Prosecutor's Office, the courts, the Ministry of the Interior, the Government of the Republic, the Parliamentary Select Committee on the Supervision of Security Authorities, the Chancellor of Justice and the National Audit Office. While external oversight is essential, our internal culture and procedures ensure that our operations are lawful and in line with the highest standards of professional ethics, sound judgement and Estonia's national security interests. We recognise the responsibility that comes with the powers entrusted to us, and we are dedicated to safeguarding the fundamental rights of Estonian residents.

The world is currently in turmoil, facing numerous threats and security challenges. Largely due to Russia's actions, further deterioration of the security environment in our region is a real possibility. Nevertheless, we can confidently affirm that Estonia is a safe country that continues to grow stronger every year.

Through close cooperation with domestic and international partners, KAPO will continue its efforts to ensure that Estonia remains secure and stable.

Margo Palloson
Director General of the
Estonian Internal Security Service
14 April 2025

DEFENDING THE CONSTITUTIONAL ORDER

The Kremlin's influence efforts aim to mobilise Russian expatriates to serve its interests and actively target young people abroad to fill the gaps in implementing its politics of division.

Employees of Russia's state-controlled media are not journalists but function as information operatives.

The primary threat to the Estonian constitutional order continues to stem from the Russian Federation's pursuit of aggressive foreign policy objectives. This threat is likely to intensify if sanctions are eased. To achieve these goals, the Kremlin seeks to undermine Western societies from within and weaken international cooperation that upholds Western values. In Estonia, these efforts have been evident not only through the routine hostile messaging of Russian media but also through various influence operations. Preventing and countering such activities is a core responsibility of KAPO.

Russia's war against Ukraine has changed the behaviour of Russian actors and individuals working in Russia's interests, as well as the strategies that Western countries, including Estonia, have adopted to pre-empt and counter Russia's hostile influence operations. Broadly speaking, propaganda-driven hostility in public spaces has decreased, but incitement and influence efforts have increasingly moved to the virtual sphere. A new and more dangerous element in these operations is the emergence of acts of sabotage, which are far more difficult to detect. Russia remains both active and aggressive. While our previous annual review focused on how Russia exploits regional marginalisation in Estonia to deepen divisions, this year's primary concern is Russia's efforts to target young people.

In Estonia, those most influenced by Kremlin propaganda tend to be older individuals, and this demographic is slowly declining. The majority of Estonia's Russian-speaking population prefers the information space and values of Estonia and the West over those of authoritarian Russia. The impact of the Kremlin's street-level political activities in Estonia has diminished due to sanctions and the relocation of activists to Russia. To further its divisive agenda and maintain its shrinking sphere of influence, the Kremlin is making a concerted effort to attract young people from neighbouring countries to events in Russia, targeting those it considers more impressionable. These individuals can later be exploited for geopolitical purposes or used to influence politics in their home countries. Although this tactic has been employed for decades, it has not produced significant success in Estonia.

After a period of reduced youth-focused propaganda events abroad due to the war, the Kremlin is once again actively offering free online and in-person programmes, competitions, excursions and Olympiads designed to lure in young participants under the guise of legitimate opportunities. These contests often present travel to Russia as a prize. However, the reality is that anyone who falls for the misleading slogans may be drawn in. It is important to remember that nothing comes without a price –

Russia will demand something in return sooner rather than later. The key tactic is digital outreach to young people, enabling direct engagement that may go unnoticed by adults.

Young people in Estonia and other countries show little interest in propaganda events that reflect Russia's interpretation of World War II. Even within Russian schools, students generally show low levels of historical interest. Consequently, Russia promotes these events both domestically and internationally by connecting them to contemporary themes – such as IT, environmental issues, media, international relations, business networks and entrepreneurship – to make them more appealing.

Youth recruitment remains a priority of the Kremlin's strategy of division, even during its ongoing war against Ukraine. Russian embassies abroad are tasked with actively pursuing this objective. For example, the Russian Embassy in Estonia promotes various youth competitions and opportunities through its media channels. In 2025, the central theme will be the 80th anniversary of the end of World War II.[1] The Kremlin aims to attract a significant number of young people from abroad to participate in its propaganda events in Russia. This effort is designed to create the illusion of international support for its war effort.

Belarus–Russia propaganda engine: The Memory Train

The Memory Train[2] is a propaganda project aimed at young people in Russia and Belarus, launched in 2022 – the year Russia began its full-scale war against Ukraine. According to the Kremlin's narrative, this initiative promotes patriotism among youth and strengthens their understanding of a shared "glorious history", with an emphasis on celebrating the Soviet victory in the Great Patriotic War, now enshrined in the Russian constitution. High school students from Russia, Belarus and other Commonwealth of Independent States countries are introduced to World War II history and given the opportunity to visit memorial sites in Russia and Belarus by train.

This year, the organisers view the project as particularly significant, as 2025 marks the 80th anniversary of the end of World War II – or, according to the Kremlin's narrative, the Soviet Union's victory. Their ambitious goal is to unite representatives from all the countries once occupied by the Soviet Union for the first time. Russian President Vladimir Putin has likened this initiative to key Kremlin propaganda campaigns, such as the Ribbon of St George campaign and the Immortal Regiment marches. Participants in the project have also met with Belarusian leader Alexander Lukashenko, a staunch supporter of Russia, who continues to remain in power despite widespread protests against his regime.

A clear example of how such projects are exploited is the way the Kremlin portrays every participant as an official representative of their home country in press releases and social media posts. The main propaganda message is framed around themes of "friendship among nations" and "world peace".

A free ticket to the Artek children's camp

In 2014, the Russian Federation occupied Ukraine's Crimean Peninsula. The following year, it launched a youth influence programme in Crimea, effectively reviving the Soviet-era tradition of pioneer camps.

1 Russia's historical narratives claim that Russia "liberated" Estonia among others from the scourge of World War II occupation. In reality, Russia occupied and repressed Estonia from the end of the war until 1991. The last Russian military units left Estonia in 1994, and the nuclear facility in Paldiski was finally handed over in 1995.

2 www.youtube.com/watch?v=SGYRZx3fvTw

At a meeting in Artek, a Wagner Group battle flag was presented to the camp's museum. Source: Artek social media account

Last year, the serious risks associated with Russian propaganda events became more apparent to the public. Unfortunately, many adults involved are still reluctant to acknowledge these issues. After the occupation of Crimea, a foundation called Sodruzhestvo, created by former participants of the Artek youth camp, announced a competition called "Artek – The Capital of Childhood" on its website. The winners included 20 delegations from around the world, among them Flamingo, a ballroom dance group based at Narva's Rugodiv Cultural Centre and led by Elena Kurgan. The prize was a free trip to Artek's 8th International Session – which was framed as an "opportunity" but actually involved sending Estonian children to a war zone.

Following the organisers' instructions, travel documents were prepared. The trip was set for the Crimean Peninsula, where, just weeks prior, missile debris from Russian military operations had fallen onto a beach, killing five people, three of whom were children.

The camp organised meetings with individuals who are under sanctions in multiple countries for crimes against peace. Among those present was Yuri Borisov, the director general of the Russian state corporation Roskosmos, as well as Russian television host Dmitry Kiselyov, who Western nations have sanctioned for spreading Kremlin propaganda in support of Russia's military presence in Ukraine. The children also attended a performance by singer and politician Denis Maidanov, whose songs often emphasise Russian nationalist themes and celebrate the VDV,[3]

3 Воздушно-десантные войска России. The Russian Airborne Forces.

OMON[4] and Spetsnaz.[5] His music videos frequently showcase tactical demonstrations, armed soldiers and military equipment. In the lead-up to Russia's invasion of Ukraine, Maidanov openly justified military aggression, declaring that Ukraine – up to the Dnipro River – belonged to Russia.

The children were kept occupied with a carefully planned schedule. They participated in the project "Bridge of Friendship: Russia and the World" and took part in MoreMedia, a programme run in collaboration with the state-owned All-Russia State Television and Radio Broadcasting Company (VGTRK),[6] which is currently under sanctions. One of the featured speakers was Russian television presenter Maria Sittel, who has previously hosted a public event supporting Russia's invasion of Ukraine.

At the camp, participants met combatants involved in attacks against Ukraine. They were shown military uniforms and weapons. At one event, a Wagner Group battle flag was handed over to the Artek Museum.

Artek organises support events for Russian soldiers fighting in Ukraine. The camp donates mattresses to frontline troops, and videos are later produced showing people in Artek camp shirts delivering aid packages.

Artek's young participants also met with war propagandist Alexander Sladkov, who has reported extensively on the Donbas conflict, documented military operations, and justified Russia's aggression against Ukraine.

Photographs published in Artek's propaganda materials show the children who travelled from Estonia arranged in the shape of the letter "V" – a symbol widely used in Russia's information war against Ukraine. The children's faces, blurred by KAPO in the materials, were clearly visible in the original Russian propaganda images. Source: Artek's social media

4 Отряд мобильный особого назначения. Special Purpose Mobile Unit, Russia's riot police force.
5 Подразделения специального назначения. Special Purpose Forces, originally Soviet-era intelligence and sabotage units; today, the term *spetsnaz* refers to various Russian special forces units.
6 Всероссийская государственная телевизионная и радиовещательная компания.

Artek and Western sanctions

On 17 July 2023, the Artek Centre was added to the United Kingdom's sanctions list due to its involvement in the Russian government's forced deportation and re-education programme targeting Ukrainian children. The UK government has stated that these sanctions will remain in place until Russia compensates Ukraine for the damage it has caused.

On 24 August 2023, both the Artek Centre and its director, Konstantin Fedorenko, were also placed under US sanctions in connection with the deportation of Ukrainian children to Russia.

On 24 June 2024, the organisation faced sanctions from multiple European Union countries as well.

Artek is a federally funded institution that operates under the directives of the Russian government and the Ministry of Education.

As Russia continues its hostile influence operations targeting young people, the Estonian government decided in 2024 to impose new sanctions to counter Russian and Belarusian influence efforts.

Under Estonian Government Sanction No 84, dated 19 December 2024, it is prohibited to organise the participation of Estonian citizens or residents under the age of 21 in events held in the interests of any Russian or Belarusian state authority, or individuals or entities affiliated with them. This applies to events taking place in the Russian Federation, Belarus, or Ukrainian territories that are illegally occupied or annexed by Russia. The ban specifically targets events that justify or endorse the aggressive policies of Russia or Belarus, their armed forces, the war of aggression against Ukraine, or the occupation and annexation of Ukrainian territories. Furthermore, it is prohibited to knowingly and directly facilitate participation in such events.[7]

7 Estonian State Gazette, www.riigiteataja.ee/akt/121122024025

The Estonian government strongly advises against travel to Russia or its occupied territories due to the risks posed by ongoing military activity. As a preventive measure, KAPO held discussions with Sillamäe youth worker Andrei Markus, who had arranged travel documents for Estonian children to attend the Artek camp. He was informed of the potential risks for both himself and the children travelling with him.

In addition to sanctions, it is essential to recognise and expose Russian influence operations to prevent the exploitation of children by a hostile foreign power. Even the participation of just one or two children in a propaganda event – whether in person or online – can be used to falsely portray a segment of Estonia's population as supportive of the Kremlin.

We urge representatives of educational and youth organisations, along with local government officials, to stay vigilant and report any hostile influence activities targeting Estonian youth by Russia or Belarus to KAPO. By working together, we can effectively counter the often covert attempts to create divisions in our society

Resettlement

In 2024, the Kremlin continued its increasingly ineffective efforts to sow division by promoting a disinformation narrative that claimed Western nations were systematically discriminating against Russian-speaking populations. This included allegations of unjustified detentions of Russian citizens and deportations on security grounds. However, these accusations are not new in Kremlin propaganda.

Similar claims have been used in the past in an attempt to influence the domestic politics of the Baltic states and exert international pressure on them, but sanctions have significantly curtailed Russia's influence within the European Union.

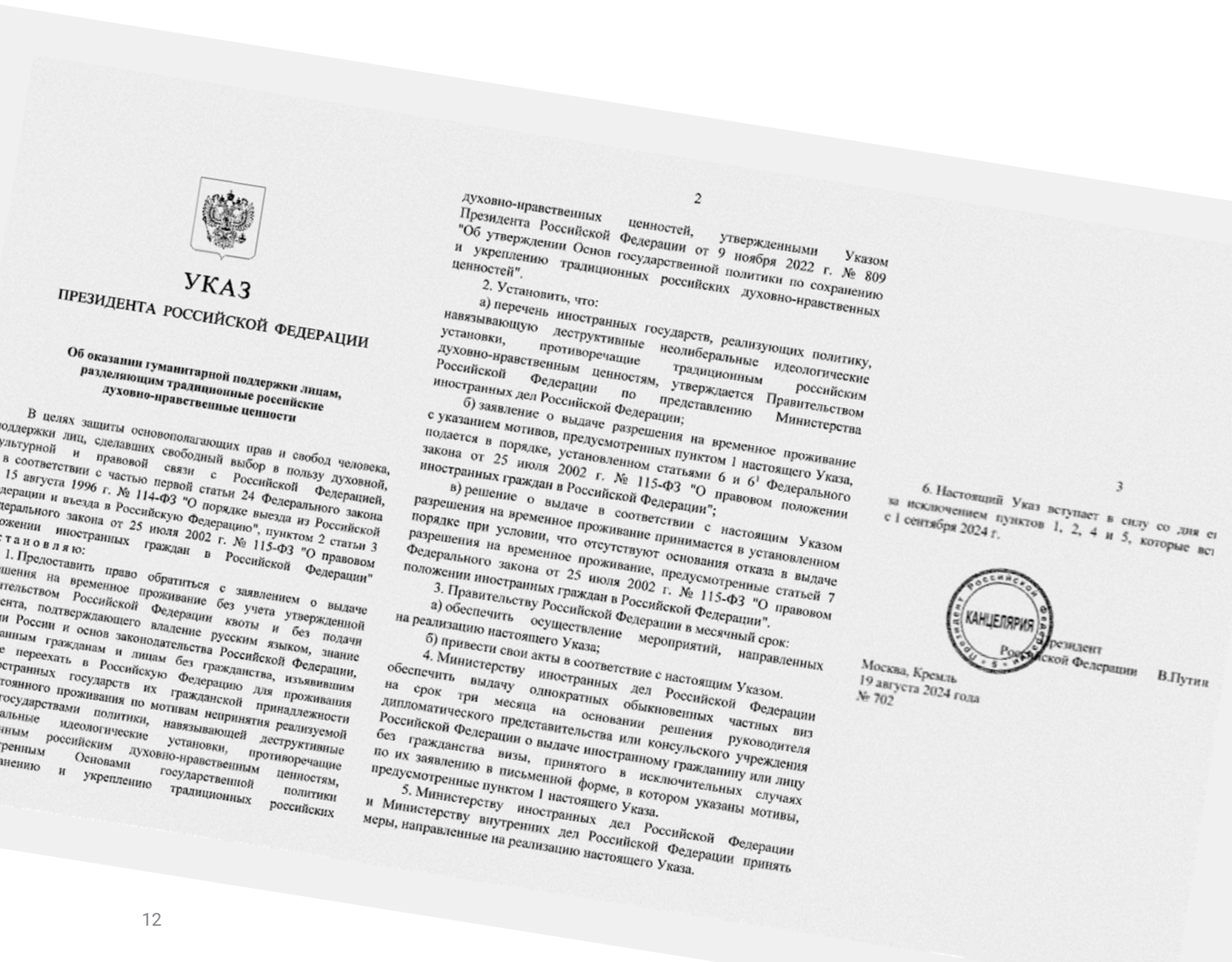
Russia's official resettlement programme has attracted little interest from residents of Western countries, primarily due to bureaucratic obstacles and a lack of consideration for the needs and preferences of prospective migrants.

In recent years, it has become evident that Russia's actual capacity or willingness to accommodate arrivals outside state-managed programmes is quite limited.

In 2024, Vladimir Putin ordered the development of proposals aimed at “guaranteeing the rights of compatriots permanently residing abroad”. The Kremlin defines the term “compatriot” both geographically and culturally, referring to individuals with ties to the former territories of the Russian Empire or the Soviet Union, as well as those connected by language, culture or Orthodox Christianity. This definition is often used to justify intervention – even military aggression – against other countries, as seen in the case of Ukraine.

The programme prioritises individuals willing to relocate to Russia because of their opposition to the policies of their current country of residence, especially those that the Kremlin describes as “destructive neoliberal ideological stances that contradict Russia’s traditional spiritual and moral values”.

The Kremlin quickly fell into its familiar patterns of self-deception. Pro-Kremlin propagandists spread false claims that thousands were about to be deported



УКАЗ
ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

Об оказании гуманитарной поддержки лицам, разделяющим традиционные российские духовно-нравственные ценности

В целях защиты основополагающих прав и свобод человека, поддержки лиц, сделавших свободный выбор в пользу духовной, культурной и правовой связи с Российской Федерацией, в соответствии с частью первой статьи 24 Федерального закона 15 августа 1996 г. № 114-ФЗ "О порядке выезда из Российской Федерации и въезда в Российскую Федерацию", пунктом 2 статьи 3 Федерального закона от 25 июля 2002 г. № 115-ФЗ "О правовом положении иностранных граждан в Российской Федерации" п о с т а н о в л я ю:

1. Предоставить право обратиться с заявлением о выдаче разрешения на временное проживание без учета утвержденной Правительством Российской Федерации квоты и без подачи документа, подтверждающего владение русским языком, знание истории России и основ законодательства Российской Федерации, иностранным гражданам и лицам без гражданства, изъявившим желание переехать в Российскую Федерацию для проживания из иностранных государств их гражданской принадлежности или постоянного проживания по мотивам непринятия реализуемой государствами политики, навязывающей деструктивные идеологические установки, противоречащие традиционным российским духовно-нравственным ценностям, Основами государственной политики по сохранению и укреплению традиционных российских

2

духовно-нравственных ценностей, утвержденными Указом Президента Российской Федерации от 9 ноября 2022 г. № 809 "Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей".

2. Установить, что:

а) перечень иностранных государств, реализующих политику, навязывающую деструктивные неолиберальные идеологические установки, противоречащие традиционным российским духовно-нравственным ценностям, утверждается Правительством Российской Федерации по представлению Министерства иностранных дел Российской Федерации;

б) заявление о выдаче разрешения на временное проживание с указанием мотивов, предусмотренных пунктом 1 настоящего Указа, подается в порядке, установленном статьями 6 и 6[1] Федерального закона от 25 июля 2002 г. № 115-ФЗ "О правовом положении иностранных граждан в Российской Федерации";

в) решение о выдаче в соответствии с настоящим Указом разрешения на временное проживание принимается в установленном порядке при условии, что отсутствуют основания отказа в выдаче разрешения на временное проживание, предусмотренные статьей 7 Федерального закона от 25 июля 2002 г. № 115-ФЗ "О правовом положении иностранных граждан в Российской Федерации".

3. Правительству Российской Федерации в месячный срок:

а) обеспечить осуществление мероприятий, направленных на реализацию настоящего Указа;

б) привести свои акты в соответствие с настоящим Указом.

4. Министерству иностранных дел Российской Федерации обеспечить выдачу однократных обыкновенных частных виз на срок три месяца на основании решения руководителя дипломатического представительства или консульского учреждения Российской Федерации о выдаче иностранному гражданину или лицу без гражданства визы, принятого в исключительных случаях по их заявлению в письменной форме, в котором указаны мотивы, предусмотренные пунктом 1 настоящего Указа.

5. Министерству иностранных дел Российской Федерации и Министерству внутренних дел Российской Федерации принять меры, направленные на реализацию настоящего Указа.

3

6. Настоящий Указ вступает в силу со дня с за исключением пунктов 1, 2, 4 и 5, которые вст с 1 сентября 2024 г.

КАНЦЕЛЯРИЯ

Президент Российской Федерации В.Путин

Москва, Кремль
19 августа 2024 года
№ 702

Путь Домой

Logo of "Put' Domoj" (The Way Home), a so-called voluntary-patriotic project that operates in collaboration with Russian state-backed funds under sanctions. Source: https://putdomoj.ru/

from the Baltic states. Russian regional authorities were instructed to prepare for the arrival of supposed mass refugees from the West. Meanwhile, Russian officials fuelled tensions in the media, suggesting that Estonia was on the verge of completely closing its border with Russia.[8] This strategy aimed to divert attention from the war in Ukraine by manufacturing new crises and amplifying them to reinforce the narrative that Russia and its citizens were facing an unprecedented – and unprovoked – assault from the West.

A larger reception centre has been established near the border in Pskov, ostensibly to assist new arrivals. Its activities include documenting alleged human rights violations against Russians abroad and recruiting volunteers for deployment to the frontlines.

At the same time, Russia's Investigative Committee announced that it would accept complaints from individuals deported from Western countries, with the stated aim of pursuing legal claims for damages where applicable.

The Kremlin has intensified its efforts to instil fear among Russian citizens by warning them that travelling abroad may expose them to widespread Russophobia. These tactics indicate a desire to revert to a closed-border system reminiscent of the Soviet Union, where entering the country was difficult, but leaving it was nearly impossible.

Several competing initiatives emerged in Russia, all seeking state support and public attention. Their central narrative focuses on providing assistance to those who are supposedly fleeing anti-Russian sentiment in the West. However, the true objective of these initiatives is to attract highly skilled specialists and individuals with specific expertise to support the Kremlin's war effort.

Logo of a project linked to Alexey Esakov, a former resident of Estonia whose residence permit was revoked due to security concerns.
Source: https://vk.com/club216564877

8 In spring 2024, Finland closed several border crossing points after months of increased migration pressure. Russia weaponised migration, with Finnish officials confirming that Russian authorities had deliberately directed undocumented asylum seekers from third countries to Finnish border crossings as part of a hybrid coercion strategy.

Sergei Neprimerov, a former Estonian resident, has now received an entry ban due to security concerns, with his residence permit revoked.
Source: Ombudsmanrf.org

Tatyana Moskalkova, Russia's Commissioner for Human Rights, met with individuals whose Estonian residence permits were revoked on security grounds.
Source: Ombudsmanrf.org

Meanwhile, Russia promises expedited relocation and documentation to those who resettle there. However, individuals may feel pressured to participate in anti-Western propaganda efforts. For some, moving to Russia simply means continuing their involvement in the Kremlin's divisive influence and propaganda networks – only now from Russian territory rather than their former country of residence.

On 16 March, during Putin's re-election, Russia's Commissioner for Human Rights, Tatyana Moskalkova, visited a polling station in Ivangorod. She met with Zoya Palyamar and Sergei Neprimerov, among others. Also present as volunteers overseeing the official confirmation of Putin's electoral victory were Sergei Chaulin and Alexey Esakov – all of whom had their Estonian residence permits revoked and are banned from entering Estonia on security grounds.

In 2024, following a recommendation from KAPO, Alexey Fedorov's residence permit was revoked due to his active involvement in pro-Kremlin influence operations in Pärnu. Fedorov utilised social media to disseminate narratives supported by the Kremlin, referring to Russia's war against Ukraine as a "special military operation". He attempted to convince his followers that welcoming Ukrainian refugees was contributing to the rise of Nazism in Estonia.

Alexey Fedorov on a several-day survival course in Russia. One of the instructors was a GRU special forces operative. Source: social media

Fedorov organised an airsoft team that trained in military tactics. Each year, he travelled to Russia to attend military exhibitions and training sessions. He openly announced that, in the event of a Russian attack, he would act in support of the aggressor state.

On the recommendation of KAPO, the Estonia Police and Border Guard Board has revoked 15 residence permits over the past three years for security reasons.

The Estonian Orthodox Church of the Moscow Patriarchate holds covert talks with Russia on funding a private school

The Russian Orthodox Church (ROC), led by Patriarch Kirill (Vladimir Mikhailovich Gundyayev), considers Estonia part of its canonical territory. This stance allows the ROC to influence religious affairs in Estonia in line with the Kremlin's aggressive foreign policy. Due to the hierarchical structure of the ROC, the Estonian Orthodox Church of the Moscow Patriarchate (EOC MP) is also affected by this influence.[9]

On 27 March 2024, during a speech at the World Russian People's Council, Patriarch Kirill referred to Russia's war against Ukraine as a holy war. This statement reflects the position of the ideological arm of the Russian regime[10] rather than a personal belief. The same can be said for his other comments about Ukraine and the positions outlined in official ROC documents that he has approved.

The Estonian government refused to extend the residence permit of Metropolitan Yevgeny (Valery Reshetnikov) on security grounds. He was appointed to lead the EOC MP following direct orders from the Moscow Patriarchate and promoted Kremlin-aligned views. Even after his expulsion, Reshetnikov continues to oversee the EOC MP remotely from Russia, further underscoring the church's deep ties to the ROC and the Moscow Patriarchate – and the local EOC MP leaders' approval of those ties.

From 1995 to 2018, Reshetnikov served as the rector of the Moscow Theological Academy, an institution for training clergy of the ROC. Similar to how the Kremlin uses the church in Russia to influence young people, Reshetnikov focused on engaging youth within the EOC MP. His goal was to cultivate a new generation of clergy who would be aligned with ROC ideology.

At his approval, the St John of Shanghai and San Francisco School (SJSFS)[11] was established in Tallinn as a private Russian-language school. The school began operating in the 2021/2022 academic year and currently has around 40 students.

After Reshetnikov's residence permit was not renewed, SJSFS attempted to downplay its connection to him. His endorsement and photograph were removed from the school's website, and he was no longer presented as the head of its governing board. Despite this, the school has continued to operate, using donations collected from EOC MP churches to support its activities.

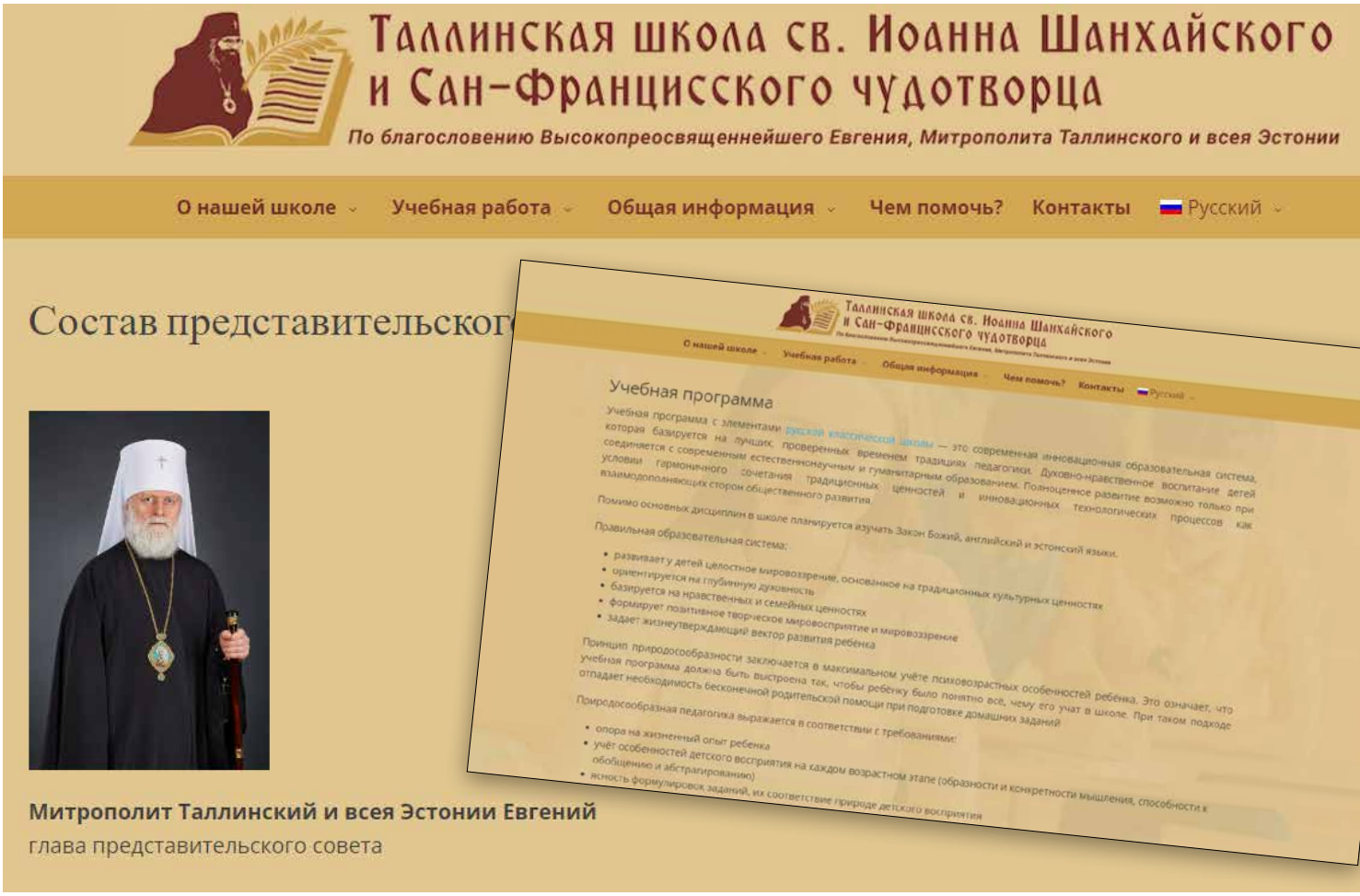
SJSFS also removed a link to the Russian Classical School website (russianclassicalschool.ru), distancing itself from this Moscow-based educational network.

The school's spiritual advisor and one of its founders is Archpriest Andrei Mere (secular name: Andres Mere). He serves as the rector of the Church of the Joy of All Who Sorrow in Tallinn.

In 2022, SJSFS hosted the Classical Education Conference, with most participants attending remotely. One of the speakers, Nadezhda Khramova, an associate professor at the Russian Orthodox University of Saint John the Theologian in Moscow, discussed the principles of Russian classical education. These principles are based on historical textbooks authored by the pioneers of Russian pedagogy, such as the 19th-century education reformer Konstantin Ushinsky and earlier scholars. The conference promoted the opposition between Russian and Western values, and highlighted the importance of instilling patriotism in children. Khramova has previously praised textbooks from the Stalin era, stating: "Thanks to Stalin, our education system still thrives! What makes Stalinist textbooks unique? They are natural and child-centred."[12]

She has also argued that textbooks from the 1940s and 1950s were superior because they employed "a modern methodology that incorporated all pre-Soviet achievements. Vladimir Potyomkin, President of the Russian Pedagogical Academy, said we had a duty to establish an education worthy of a victorious nation – as early as 1943!"[13]

As a state-recognised private school, SJSFS receives government funding from Estonia's national budget. However, despite this funding and the rejection of Reshetnikov's residence permit, both EOC MP and SJSFS representatives have actively sought alternative financing, including through legally questionable means.



Source: sjk.ee

In 2024, EOC MP representatives engaged in negotiations for funding with Rossotrudnichestvo, a Russian federal agency under the jurisdiction of the Russian Foreign Ministry. This agency supports Russia's influence projects and serves as a key tool for the Kremlin's aggressive foreign policy. It coordinates organisations and individuals that support Russia's foreign and security policy objectives and disseminates pro-Kremlin narratives globally. Since 2022, Rossotrudnichestvo has been under EU sanctions due to activities that undermine or threaten Ukraine's territorial integrity, sovereignty and independence.

To circumvent scrutiny and funnel sanctioned Russian funds into Estonia, the EOC MP has explored various financial schemes. For example, while residing in Russia, Metropolitan Yevgeny personally petitioned Patriarch Kirill to approve the establishment of a charitable fund in Russia aimed at raising money for SJSFS.

9 As of 31 March 2025, the Estonian Orthodox Church of the Moscow Patriarchate is officially registered under its new name, the Estonian Christian Orthodox Church.
10 The designation of the war of aggression as a "holy war" was condemned by the Parliamentary Assembly of the Council of Europe (PACE). In April 2024, PACE adopted a resolution criticising Patriarch Kirill, describing the ROC as an ideological arm of Vladimir Putin's regime, complicit in war crimes.
11 This is not to be confused with St John's School (Püha Johannese Kool), which also operates in Tallinn.
12 www.youtube.com/watch?v=KP46KcXDblU, see at 09:21.
13 www.youtube.com/watch?v=8RaMPi9MO6s, see at 19:28.

On 17 June 2024, the St John of Shanghai Charitable Foundation was officially registered in Russia.[14] The foundation's director, Dmitry Mikhailovich Yefremenko, has a longstanding connection to the EOC MP. Although currently based in Russia, he was previously a board member of the Joy of All Who Sorrow Parish in Tallinn from 2004 to 2011.

Following Metropolitan Yevgeny's example, SJSFS also celebrates significant Russian state holidays, including Victory Day on 9 May.

On 10 May 2023, SJSFS's Director Denis Polikarpov attended a memorial service at the Bronze Soldier monument at Tallinn's Defence Forces Cemetery. The service, organised by the EOC MP, was led by SJSFS's spiritual advisor, Archpriest Andrei Mere, along with other EOC MP clergy. Mere's wife, Jelena Mere, who leads the school's Orthodox Culture Club, also attended.

9 May remains an important date for other EOC MP clergy as well. In previous years, Metropolitan Yevgeny personally participated in Victory Day memorial services at the Bronze Soldier monument.

Furthermore, EOC MP clergy have taken part in the Immortal Regiment campaign, which the Kremlin considers one of its most successful foreign influence initiatives. This campaign serves as a vehicle for promoting Russian historical narratives. For example, in 2020, Archpriest Oleg Vrona, rector of the Church of St Nicholas the Wonderworker in Tallinn, participated in the online version of the Immortal Regiment march, which was broadcast on Spas (Спас), the official television channel of the ROC.

After Russia invaded Ukraine in 2022, YouTube blocked Spas. As of December 2023, the channel has been under EU sanctions.

14 Благотворительный Фонд «Святителя Иоанна Шанхайского», ID 5027329440.

The head priest of St Nicholas Church, Oleg Vrona, appears in the online version of the Immortal Regiment on the ROC television channel Spas. Source: YouTube

Source: Facebook, Lilian Kerro

EU sanctions curb hostile propaganda

Alongside rapid technological advancements and global developments that erode societal security, social media is playing an increasingly prominent role in influence operations.

For Russia, media-driven influence operations are among its most valued strategies.[15] In addition to its domestic propaganda, the Kremlin has directed substantial resources to create divisions within Western societies. In recent years, these efforts have particularly focused on undermining public and political support for Ukraine. In response, the European Union has imposed international sanctions on Russian state-controlled propaganda channels since 2014, due to their support of Russia's aggression against Ukraine. However, these restrictions alone are not effective unless they are strictly enforced. Estonia has effectively implemented EU sanctions since 2019 and intensified these efforts following Russia's full-scale invasion of Ukraine in 2022. Sanctions are a long-term measure, and research conducted between 2022 and 2024 confirms that curbing propaganda has had a tangible impact.

To be effective, sanctions require strong enforcement measures, including holding violators accountable. On 27 January 2025, the Harju County Court convicted Mati-Dmitri Terestal, a former executive of Sputnik Estonia. However, the verdict has not yet entered into force. Another leader from Sputnik Estonia, Elena Cherysheva, fled the country and now serves as the head of Sputnik's operations in Crimea, continuing her role in Kremlin propaganda. She remains internationally wanted on suspicion of violating international sanctions.

Legal proceedings have been concluded against Svetlana Burceva, an employee of Sputnik and its affiliate Baltnews, both part of the Russian state-controlled media conglomerate Rossiya Segodnya. A court ruling is expected in June 2025. Burceva faces charges for violations of sanctions and actions against the state. She authored a book on hybrid warfare, published by the Russian private intelligence firm R-Techno, whose owner and CEO, Roman Romanchev, is a former FSB officer. The book, which echoes the Kremlin's hostile narratives, presents hybrid warfare as a struggle for the world's future, one that Russia must ultimately win.

15 Russia's media propaganda spending is at an all-time high, https://euromaidanpress.com/2024/10/07/russia-to-spend-118-million-per-month-on-state-propaganda-in-2025/?utm www.moscowtimes.ru/2024/10/07/26-milliarda-rublei-vnedelyu-rossiya-uvelichit-rashodi-nagospropagandu-donovogo-istoricheskogo-rekorda-a144152

16 Public Opinion Monitoring Survey (13–19 December 2024), www.riigikantselei.ee/uuringud?view_instance=0&current_page=1

EU sanctions have restricted access to 53 Russian TV channels and 307 websites in Estonia, according to the country's media regulator, the Consumer Protection and Technical Regulatory Authority. Research indicates that increased oversight and accountability measures, in response to security concerns following Russia's invasion, have significantly diminished the influence of these channels in inciting hatred over the past two years.[16]

However, limiting sanctioned propaganda on social media remains a complex challenge. Despite restrictions, sanctioned individuals and Kremlin-controlled media continue to reach large audiences through YouTube and Telegram. While official accounts are often shut down, new ones quickly emerge, re-attracting viewers' attention. Notably, Kremlin propagandists – who once primarily targeted Estonia's Russian-speaking community through official Kremlin media – have now become increasingly visible on social media.

Russian extremists who supported the 2014 occupation of Crimea and operated in the Baltic states continue to serve the Kremlin's propaganda machine from within Russia. They have discovered alternative platforms, including the video channel of former Latvian MEP Andrei Mamykin (Andrejs Mamikins). In February 2025, YouTube shut down Mamykin's channel for featuring sanctioned individuals who were seeking alternative outlets after Russia's propaganda channels had been blocked. Mamykin has since launched a new channel.

In addition to state authorities, platform users can also report sanctioned channels. Media platforms are responsible for ensuring that Kremlin propaganda channels, which are under EU sanctions, are not disseminated. Moreover, we want to remind our readers that enabling access to sanctioned channels may result in criminal liability, since providing services to sanctioned individuals grants them economic resources.

Estonia is far from the only country that classifies violations of international sanctions as a criminal offence. Since this issue impacts the enforcement of EU law, the European Union is currently discussing the harmonisation of criminal law to ensure sanctions imposed by the EU are enforced uniformly across all member states.

Kremlin journalists participate on the frontlines in roles indistinguishable from those of combatants. Source: Pervõi Kanal

Kremlin propaganda is not journalism

In a democratic society, any restrictions on fundamental rights must be lawful, constitutional and proportionate. This principle applies to freedom of expression, which in free societies involves the recognition of the need to tolerate content that may be unpleasant or disturbing. While Western democracies view a free society as a strength, Russia perceives it as a weakness that it seeks to exploit.

Employees of Russian state-controlled media, particularly those in leadership positions, have compared their work to that of a Ministry of Defence department.[17] During peacetime, they establish trust and cultivate an audience that can be mobilised when necessary. The extent to which a state allows itself to be targeted in information warfare, and what measures it considers appropriate to mitigate such attacks, largely depends on security conditions and public perception. In many countries, Russian media operatives masquerade as journalists and continue to operate with minimal restrictions; however, this is not the case in Estonia.

Russia ranks among the lowest in the world for press freedom, while Estonia ranks among the highest.[18] Usually, the journalistic community itself, both in Estonia and internationally, determines who belongs to the profession. In certain legal and security contexts, authorities may need to assess whether individuals involved in influence operations that indirectly threaten national security should be treated differently from the general public – let alone whether they should be recognised as journalists.

In contrast to Russia, where scrutinising government decisions or expressing criticism can endanger journalists and their families, Estonian journalists can operate without such risks. In democratic societies, journalists serve as watchdogs, and the government does not interfere with their work or restrict their freedom of expression unless there are overriding constitutional reasons to do so. In Russia, independent journalists face imprisonment, censorship and denial of access to broad audiences, or are forced to flee the country to safeguard their lives. Media outlets with significant reach, along with individuals who identify as journalists, often adhere to state directives and take pride in being labelled by the Ministry of Defence as a weapon.[19] This makes them information warriors.

The security risks posed by Russian influence operations may often be indirect and manageable in each individual instance, but their long-term, systematic

17 https://euvsdisinfo.eu/chief-editor-rt-is-like-a-defence-ministry
18 https://rsf.org/en/index
19 Archived Interfax news article, https://web.archive.org/web/20160520021300/https://interfax.com/newsinf.asp?id=581851

nature threatens national security by exacerbating societal divisions. For years, the most vulnerable target group in Estonia was its Russian-speaking population, while Estonian speakers were effectively shielded. However, advancements in artificial intelligence (AI) are changing the threat landscape. Today's AI tools can produce fluent Estonian-language content that incites hatred, while the ongoing development of AI applications makes disinformation increasingly convincing.

More and more, institutions, media outlets and individual consumers are struggling to distinguish between genuine opinions from Estonian users and coordinated Russian information campaigns. This growing challenge highlights the importance of source verification by newsrooms and the need for media literacy among the public. It is crucial to prevent Kremlin influence operations from gaining traction in Estonia.

Propagandists impersonate journalists using press kits.
Source: Estonian Internal Security Service

Harassment of Estonian officials

The Kremlin is trying to undermine support for Ukraine while reinforcing its historical narrative by intimidating decision-makers in Western societies. Estonia and its allies have taken firm action to curb Russia's influence, causing significant frustration in the Kremlin – a clear indicator that these efforts are effective. One of Russia's most sensitive issues has been the removal of Soviet-era monuments – which the Kremlin considers territorial markers – in other countries. To intimidate and pressure foreign officials, Russia has initiated politically motivated criminal cases against members of EU governments, including those of the Baltic states, for participating in the removal of Soviet occupation monuments or for their support of Ukraine.

The Russian Investigative Committee publicly announced in absentia charges against nearly 200 individuals, including former Estonian Prime Minister Kaja Kallas, former State Secretary Taimar Peterkop and former Minister of the Interior Lauri Läänemets, Member of Parliament Urmas Reinsalu, and former Police Chief Elmar Vaher. This marks a departure from previous years, as Russia had not used such intimidation tactics against high-ranking foreign politicians before.

For the past two years, on 9 May, a banner reading "Putin. War criminal"[20] has been displayed on the Narva Museum building facing Ivangorod on the Russian side. Russia's response to this action has revealed the true nature of its regime. In the summer of 2024, the Basmanny District Court in Moscow issued an in-absentia arrest order for the director of

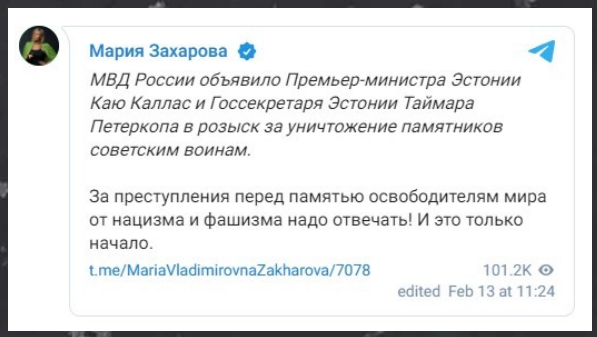
20 On 17 March 2023, the International Criminal Court (ICC) issued arrest warrants for Russian President Vladimir Putin and Presidential Commissioner for Children's Rights Maria Lvova-Belova, suspected of unlawfully resettling Ukrainian children from occupied Ukraine to Russia as a war crime.

The photo shows the car window of Minister of the Interior Lauri Läänemets, damaged in a hybrid attack in December 2023.
Source: Police and Border Guard Board

Narva Museum, initiating a politically motivated criminal case for allegedly spreading "false information" about the Russian military as part of a politically driven group. This case exemplifies how Russia extends its aggression beyond Ukraine, using legal harassment and intimidation to target free societies.

By fabricating criminal cases against foreign politicians and officials, the Kremlin weaponises the legal system to harass and deter decision-makers from taking further measures to counter the Russian threat – both within their own countries and in support of Ukraine.

Although Lenar Salimullin, Russia's temporary chargé d'affaires in Estonia, promised a written response regarding Moscow's decision to place Estonia's prime minister and other officials on a wanted list, Estonia's Ministry of Foreign Affairs has yet to receive it.



A post by Maria Zakharova, spokesperson for the Ministry of Foreign Affairs of the Russian Federation, reads: "The Ministry of Internal Affairs of Russia has declared Estonian Prime Minister Kaja Kallas and State Secretary Taimar Peterkop wanted in connection with the destruction of Soviet soldier memorials. Those responsible for crimes against the memory of the liberators of the world from Nazism and fascism must be held accountable. And this is just the beginning!" Source: Telegram

COUNTERINTELLIGENCE

Russia's aggressive methods are the new reality.

For decades, Russian special services have exploited the principle of academic freedom in democratic countries, cynically using it for their intelligence and influence activities.

China, facing a slowing economy and a deteriorating global image, is shifting its focus from political and security issues to soft power values.

The past year has been characterised by hybrid threats and acts of sabotage originating from the Russian Federation. These hybrid operations involve various forms of attack that occur simultaneously to varying degrees, all with the common goal of forcefully imposing Russia's will. These attacks go beyond simple vandalism, such as breaking car windows or defacing monuments; they can also include cyberattacks, influence operations, arson, assassinations, coup attempts and more.

Since the beginning of Russia's full-scale war against Ukraine, its non-military operations in the West have become more aggressive and overt. Russia aims to spread confusion and fear beyond its borders while draining Western resources. Ultimately, its overarching goal is to undermine support for Ukraine.

In early 2024, the GRU,[21] Russia's military intelligence, attempted to intimidate Estonian politicians and public figures who had been particularly vocal in supporting Ukraine. The attacks included vandalism against the vehicles of the interior minister and a journalist, as well as the destruction of World War II memorials. The perpetrators had a longer list of targets and broader plans, but KAPO quickly identified the perpetrators and thwarted attacks against more than ten individuals, along with other planned operations designed to amplify their impact.

Although the publicly disclosed cases disrupted further attacks, similar operations cannot be ruled out in the future.

Around ten individuals were arrested in connection with these hybrid attacks. An Estonian court sentenced GRU operative Allan Hantsom to six years and six months in prison for committing a crime against the state.

While some suspects remain in Russia, they have been placed on international wanted lists and are barred from entering the Schengen Area for years to come. Should they travel to a country with values similar to Estonia's, they will be apprehended.

Two of these individuals are already known to the public: Alik Khuchbarov and Ilya Bocharov.

21 GRU – the Russian foreign military intelligence agency, commonly known as the Main Intelligence Directorate, or Главное разведывательное управление.

Alik Yuryevich Khuchbarov (Хучбаров Алик Юрьевич)

Born 12 November 1992, citizen of Estonia and Russia; residences: Pskov, Pechory and Luki, Russia

In 2012, Alik Khuchbarov obtained information for the FSB[22] about the professional activities of Estonian police officers at the Piusa border checkpoint and individuals within the social circles of the police officers.

In 2016, Khuchbarov was convicted for collaborating with the FSB. The court sentenced him to three years in prison.

In the hybrid attacks carried out in 2024, Khuchbarov worked for the GRU.

Ilya Sergeevich Bocharov (Бочаров Илья Сергеевич)

Born 29 June 1991, citizen of Russia; residence: Saint Petersburg, Russia

Ilya Bocharov is associated with the African Initiative information agency, which is involved in influence operations supported by Russian intelligence services. The African Initiative is a platform managed by the GRU; it disseminates disinformation about the United States and European countries.

The deputy head of the African Initiative, Maxim Reva, was one of the agitators during the Bronze Night events in Tallinn in 2007 and a member of the Night Watch (Nochnoy Dozor) group. Reva received the "For Crimea" medal in recognition of his involvement in Russia's hybrid operation in Ukraine in 2014. He has been actively involved in the operations of Kremlin propaganda channels, spreading disinformation and hostile propaganda and inciting hatred.

If you encounter these individuals or have any information about them, please contact KAPO.

22 FSB – Russian counterintelligence agency, officially known as the Federal Security Service, or Федеральная служба безопасности.

Stills from the video that led to the treason conviction. Source: Telegram

In February 2024, Andrey Makarov set fire to a car with Ukrainian licence plates on Mõisavahe Street in Tartu. He attempted to frame the act as the work of the movement KOOS by painting the word "KOOS" in large letters on the car's bonnet. The burning vehicle was then filmed, and the footage was uploaded to Telegram, where thousands of users watched it. The objective was to divide Estonian society, sow fear and undermine public trust. Through cooperation with partner agencies, KAPO determined that, in addition to setting the vehicle ablaze, Makarov had been monitoring a Russian Air Force pilot living in Lithuania, NATO allied forces' equipment in Riga, and police and emergency services activities in Poland.

Makarov holds dual citizenship. When he reached adulthood, he applied for and obtained Estonian citizenship through ancestry. However, six years later, he joined a GRU special forces, or Spetsnaz, unit. Acting in the interests of both the FSB[22] and the GRU, he communicated using phone calls, applications and in-person meetings. As a dual citizen, he exploited his Estonian passport and Schengen privileges for free movement.

In early 2024, the Battle of the Blue Hills memorials near Sillamäe were vandalised. Under the cover of night, paint was poured on the memorials, the act was filmed, and the perpetrators left the scene. Source: Estonian Police and Border Guard Board

On 25 March 2025, the Tartu County Court convicted Makarov of treason and sentenced him to 15 years in prison. The decision has not yet come into force.

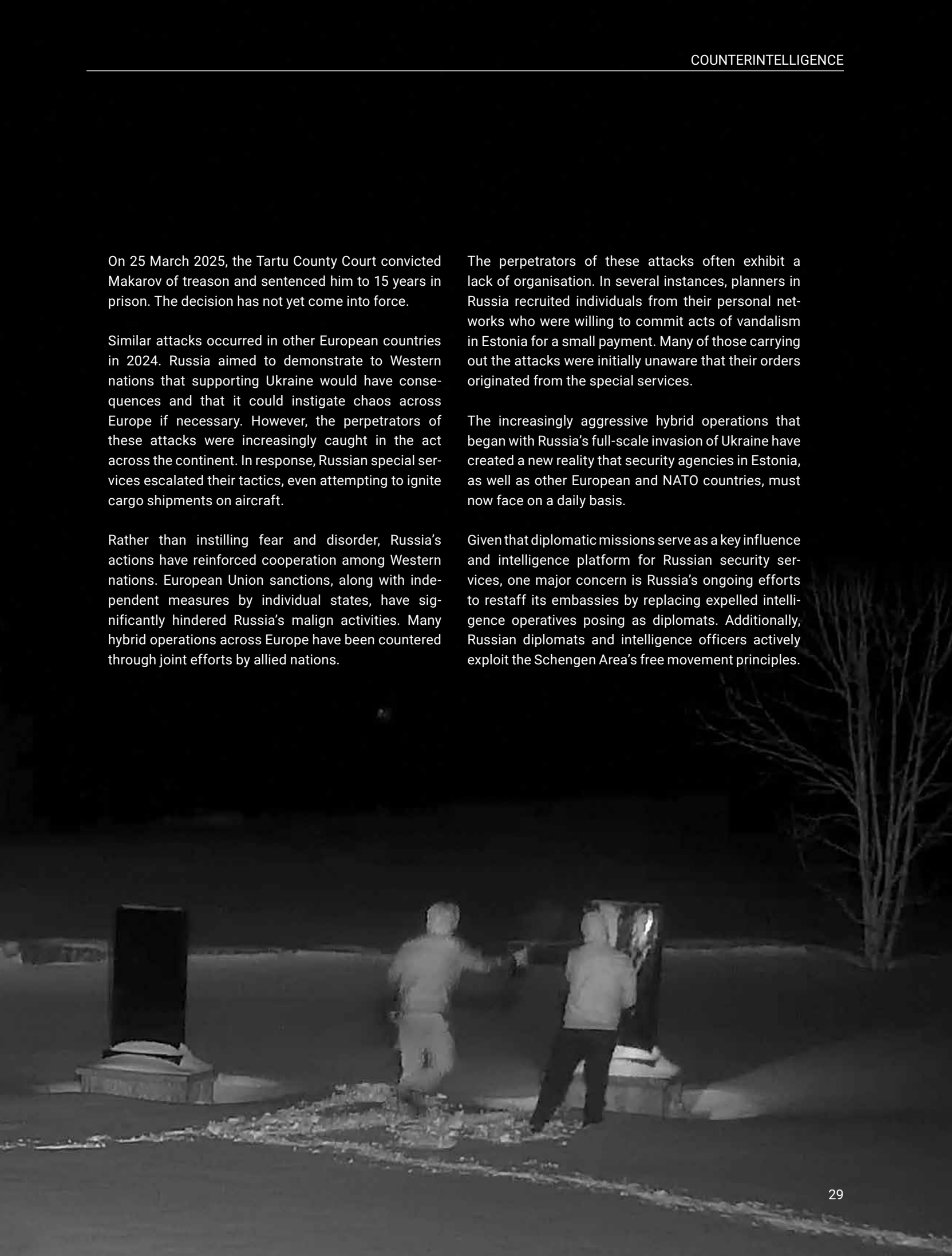
Similar attacks occurred in other European countries in 2024. Russia aimed to demonstrate to Western nations that supporting Ukraine would have consequences and that it could instigate chaos across Europe if necessary. However, the perpetrators of these attacks were increasingly caught in the act across the continent. In response, Russian special services escalated their tactics, even attempting to ignite cargo shipments on aircraft.

Rather than instilling fear and disorder, Russia's actions have reinforced cooperation among Western nations. European Union sanctions, along with independent measures by individual states, have significantly hindered Russia's malign activities. Many hybrid operations across Europe have been countered through joint efforts by allied nations.

The perpetrators of these attacks often exhibit a lack of organisation. In several instances, planners in Russia recruited individuals from their personal networks who were willing to commit acts of vandalism in Estonia for a small payment. Many of those carrying out the attacks were initially unaware that their orders originated from the special services.

The increasingly aggressive hybrid operations that began with Russia's full-scale invasion of Ukraine have created a new reality that security agencies in Estonia, as well as other European and NATO countries, must now face on a daily basis.

Given that diplomatic missions serve as a key influence and intelligence platform for Russian security services, one major concern is Russia's ongoing efforts to restaff its embassies by replacing expelled intelligence operatives posing as diplomats. Additionally, Russian diplomats and intelligence officers actively exploit the Schengen Area's free movement principles.



Russian special services' activities at the border

Since the beginning of Russia's full-scale war, its special services have adopted increasingly aggressive recruitment tactics. The FSB, which has control over visas and border crossings, closely monitors individuals entering Russia. Travellers crossing the border may have their communication devices inspected or their contents copied by the FSB.

Since 2023, the FSB has periodically required incoming travellers to complete an additional paper questionnaire that requests detailed contact information. This appears to be an attempt to facilitate future surveillance. Individuals are also compelled to disclose, in writing and with their signature, whether they have acquaintances working in Estonian security services, their views on the European Union and Ukraine, and whether they know anyone directly involved in the war on Ukraine's side. Many visitors to Russia find themselves in a "no-win" situation – whether they answer these questions truthfully or are caught withholding information, they risk facing pressure from the FSB, to divulge information about themselves and their relatives.

The Estonian government strongly advises its citizens against travelling to Russia, as it is unable to assist anyone who finds themselves in danger.

If you have had contact with foreign intelligence services, have been approached for recruitment, have come under the influence of a hostile foreign intelligence service, or have knowledge of offers of cooperation or sabotage plans, please contact the Estonian Internal Security Service at kapo@kapo.ee or info24@kapo.ee. Recruitment attempts often span years and may not be immediately apparent, which is why it is important to report even isolated contacts. There is a way out, no matter how inescapable the situation may seem.

A GRU operative

In June 2024, the Harju County Court convicted Vyacheslav Morozov, a Russian citizen and lecturer at the University of Tartu, for acting on behalf of a foreign intelligence service against the Republic of Estonia. He was sentenced to six years and three months in prison.

Morozov's collaboration with the GRU began in the early 1990s when he was recruited as a student at Saint Petersburg State University. However, he became truly valuable to the GRU when he successfully secured a position at the University of Tartu through an international competition.

The GRU did not interfere in Morozov's academic work; he was free to express his opinions as a lecturer and researcher, including criticising Russian policies if he chose to. What made him valuable to the GRU was his extensive international network in academia and

the contacts he maintained. Morozov gathered and shared information on how Russia's actions were perceived in Estonia and how Estonian–Russian relations were interpreted.

Morozov's case was not unique. Russia's special services have continued operating within Russian universities much as they did during the Soviet era. All three of Russia's major intelligence agencies – the FSB, the GRU and the SVR – remain actively engaged in domestic academic institutions. Their activities mainly fall into two categories: counterintelligence, led by the FSB, and intelligence gathering, in which all three services participate. At times, counterintelligence efforts can escalate into outright intelligence operations.

Russian universities employ undercover officers,[23] primarily within their human resources and international cooperation departments. Primarily within their human resources and international cooperation departments – key areas where intelligence-relevant information can be gathered. Western countries often underestimate the systematic and large-scale nature of intelligence operations within Russian academia.

A notable example of the mindset of the Russian special services is a set of recommendations on international collaboration adopted in 2019, which required Russian researchers to notify authorities five days in advance of any in-person meetings with foreign academics. After such meetings, they were also required to submit reports detailing not only the names of participants but also the exact meeting location, including room numbers. Researchers engaging with foreign colleagues had to be approved by their institution's leadership. No Russian academic was permitted to meet a foreign counterpart alone. Although these recommendations were repealed a year later, they reflected a worldview of the special services that fundamentally conflicts with the Western principle of academic freedom.

For decades, Russia's special services have exploited the principles of academic freedom in democratic countries to advance their own intelligence and influence operations.

The special services in Russia monitor both their own citizens and foreign students and lecturers who arrive in the country. When it comes to monitoring their own nationals, these agencies focus on four main objectives: recruitment, counterintelligence, surveillance of Russian citizens, ideological monitoring (which is becoming increasingly important), and intelligence gathering. Morozov fell into the last category; he was drawn into long-term cooperation because he was viewed as a promising social scientist with an extensive international network.

Russian special services are particularly interested in foreign nationals attending Russian universities. Almost all international research collaborations, as well as foreign students and lecturers at these institutions, are closely monitored. The level of scrutiny increases with the university's prominence. These agencies collaborate effectively, as there is a substantial pool of students and academics available for potential recruitment.

Intelligence recruitment efforts within universities are a long-term endeavour. Throughout a student's academic career and subsequent professional life, there is ample time to observe potential recruits, introduce controlled interactions into their social circles, and gradually initiate the recruitment process. What matters is not who the student is at present but who they may become in the future. These recruitment efforts are typically subtle rather than aggressive. A slow and deliberate web is woven around the target, making it increasingly difficult for them to withdraw. Often, the recruit is unaware of what is happening until it is too late.

23 Intelligence officers are officially employed bythe academic institution, but in reality, they continue to work for the intelligence agency.

China's tarnished image

The public image of the People's Republic of China in Estonia has recently deteriorated for several reasons. Key factors include its support for Russia, the aggressor state in the ongoing war in Ukraine; the involvement of a Chinese vessel in damaging the Balticconnector gas pipeline and telecommunications cables; and ongoing threats from China against Taiwan.

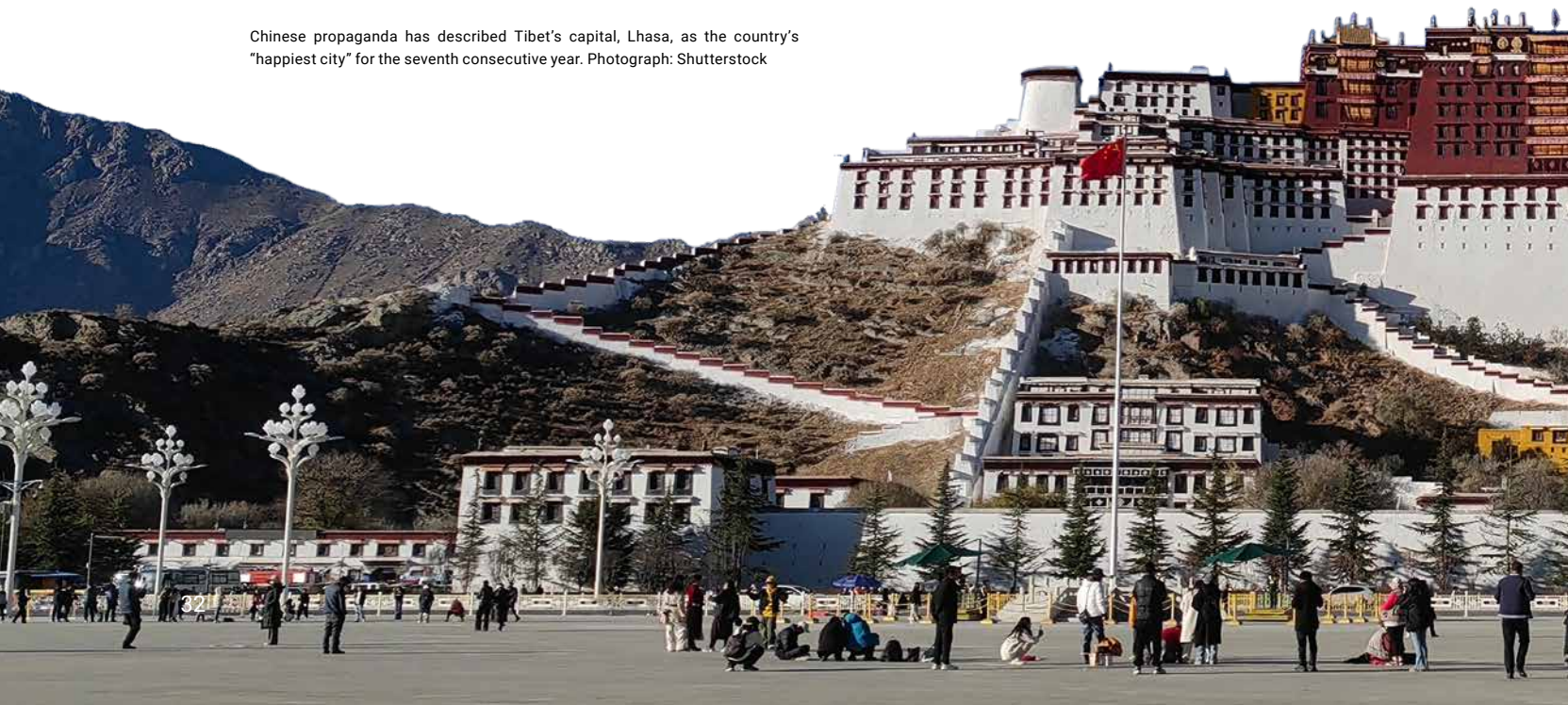
In response, the Chinese Embassy in Estonia has intensified its efforts in soft power initiatives, focusing on media, culture, education and sports. These efforts primarily target local municipalities. The embassy has organised frequent visits to local educational institutions, particularly Russian-language schools in Ida-Viru County. Additionally, the embassy has engaged with local officials and politicians, who tend to be more open to Chinese influence than those at the national level. In 2025, China introduced temporary visa-free travel for Estonian citizens.

While such activities are not prohibited, it is important to understand their purpose and methods. The primary goal is to improve China's image and strengthen its economic ties through influence operations.

China is attempting to revitalise its slowing economy and repair its increasingly tarnished reputation by diverting attention away from political and security issues while emphasising soft power. To achieve this, it organises visits and cultural trips to China for politicians, officials, journalists and educators, in an attempt to use their voices to subtly promote its image.

In autumn 2024, the Finnish public broadcaster YLE's investigative programme MOT reported on a journalist from the Chinese newspaper *Guangming Daily* who had ties to Chinese intelligence and had been active in Finland and Sweden. Few people know that this journalist's predecessor – the newspaper's previous correspondent in Finland – also visited Estonia in 2019. During that visit, the correspondent interviewed both a member of the Estonian parliament and a researcher at the International Centre for Defence and Security (ICDS). Although China currently has no resident journalists in Estonia, occasional visits from Finland or Latvia are not uncommon. For example, in November 2024, a correspondent from China's state news agency *Xinhua* visited Estonia to cover a delegation of Chinese Tibet experts endorsed by the Communist Party, who were invited to Tallinn by the Chinese Embassy. In Tallinn, the embassy also hosted a seminar on Tibet,

Chinese propaganda has described Tibet's capital, Lhasa, as the country's "happiest city" for the seventh consecutive year. Photograph: Shutterstock



where Chinese experts spoke about human rights, freedom, and the Communist Party's contributions to Tibet's development. The talking points from this seminar were later featured in a propaganda article published on 12 November 2024 by MK Estonia.[24] China has previously sought and will continue to pursue media coverage in Estonia, including through paid content marketing articles placed through local intermediaries. This trend is once again on the rise.

Beyond the media narrative, China also exploits the local Chinese community to advance its interests. This includes organisations like the Chinese Compatriots Association in Estonia. Recently, the Chinese Embassy has begun recruiting "consular volunteers", a tactic already widely implemented elsewhere in the world. This initiative is part of the Communist Party's United Front Work Department (UFWD), which China employs to gather intelligence, conduct influence operations and even harass dissidents abroad.

A small country cannot afford to develop dependencies on authoritarian regimes in any sector. China has never been aligned with the West, and its current trajectory indicates that this is unlikely to change. Therefore, it is essential to view China through a security lens, especially given that China itself approaches all areas of governance through the prism of the state security and Communist Party apparatuses' grip on power.

Leaders of the Chinese community in Estonia with the ambassador and consul holding a banner with the inscription: "The embassy is a window that conveys love for the homeland and shields the body and soul of its compatriots." Photograph: Chinese Embassy in Estonia

24 www.mke.ee/kontent-marketing/tibet-sekret-uspekha

PROTECTION OF STATE SECRETS

An increasing number of people and companies are handling classified information as national defence grows in importance.

KAPO conducted nearly 60 training sessions for 1,800 participants in 2024 to strengthen security culture and risk awareness.

The growing interest of the Estonian business sector in participating in classified security, research and development projects offers companies valuable experience while promoting innovation within Estonia's security and research landscape. However, this trend poses challenges for government agencies. While many European countries have well-established risk management frameworks for critical national projects, including classified procurements, Estonia has relatively limited experience with large-scale initiatives involving industrial security.

Authorities need to swiftly adapt to these changes and review the existing legal framework to ensure that companies understand their rights, obligations, and responsibilities. A more explicit framework may also be needed to assess which companies are qualified to participate in these projects.

Various international projects, particularly classified European Union and NATO projects, inevitably attract malicious foreign interest. Therefore, it is essential to provide companies and their employees with ongoing advice and training to enhance their threat awareness. Most businesses are unfamiliar with handling classified information, and their employees often lack prior experience in this area. This makes KAPO's systematic preventive work even more critical. Establishing a well-structured security culture within companies strengthens their overall resilience and ensures better protection in day-to-day operations.

In 2024, we conducted nearly 60 training sessions with approximately 1,800 participants.

Security vetting

A security clearance is required to access state secrets, and this process is necessary to determine the potential presence of grounds for denial, including evaluating the trustworthiness of individuals tasked with security-sensitive roles. However, there is often limited discussion about how these security checks are conducted and what individuals can expect to undergo during the process. To gain some insights, we consulted a security vetting officer.

The security vetting process generally takes three months, sometimes longer. Why does it take so long?

A significant amount of time is spent preparing inquiries to other institutions and waiting for responses.

Once the information is received, we start piecing together whether the individual's self-disclosed data matches other sources. We prepare questions for the security interview and may also speak with colleagues and acquaintances who know the person.

Some applications take longer to process. This may be due to the applicant's investment activities, crypto-currency transactions, past frequent travel to Russia or other factors.

What does invasion of privacy mean in the context of security vetting?

Inevitably, we examine very personal information – details that are not public and that individuals would not usually share with outsiders. The degree of intrusion is strictly limited to what is necessary to identify potential grounds for refusal. We handle all information with respect, whether provided in documents or during interviews. The information is securely stored and not shared beyond this process. The procedure is also familiar to us as vetting officers because we undergo the same process ourselves.

Some people, especially those undergoing their first interview with KAPO, may feel nervous. What should they expect?

To put it simply, we start from the very beginning. We ask a lot of questions, including some uncomfortable ones. We understand that opening up about one's life to a stranger is unpleasant. That is why we ensure a professional and non-judgemental environment when assessing an individual's trustworthiness. Before the

interview, we explain where to go, what to do, what to bring and where to find additional information. The average interview lasts three to four hours, but some can take much longer. If necessary, we take breaks, including lunch breaks for longer sessions.

During interviews, people are sometimes startled that we take detailed, even word-for-word, notes. This is necessary to protect the individual, as they can review the transcript and request clarifications or corrections if needed.

Has anyone ever withdrawn their application after the interview?

There have been cases where an employer informs us that an individual has requested to withdraw their application – even when nothing seemed problematic during the interview. However, there are also instances where we uncover debts, tax fraud or undeclared income, from cryptocurrency or rental earnings, and the person then chooses to withdraw their application rather than discuss the matter further. Applications have also been withdrawn due to excessive alcohol consumption or drug use when the individual is unwilling to change their habits.

If someone is having financial difficulty, does that affect their chances of obtaining a security clearance?

If we find that a person is struggling with financial obligations, the impact depends on the extent of their debts. High-interest payday loans or living significantly beyond one's means are particularly concerning.

During the process, we assess whether the individual has a clear plan to reduce their debt and improve their financial situation. If they show no intention of doing so and continue to take out new loans, this could indeed be a problem. The person could become vulnerable to influence or coercion.

Sometimes, we offer guidance on improving financial stability and later review whether the individual has followed the advice. In some cases, we may grant a clearance for a shorter period as a form of probation. Refusal is always a last resort.

How do you assess potentially risky habits or addictions in the vetting process?

Addiction requires a medical diagnosis, and it is a serious matter. It can impair judgement, compromise a person's sense of responsibility and make them susceptible to manipulation. We have noticed that younger generations often fail to perceive the risks of drug use. We have a zero-tolerance policy towards active drug users, including so-called casual users. With the individual's consent, we may also require an official drug test. This is a sensitive and complex issue.

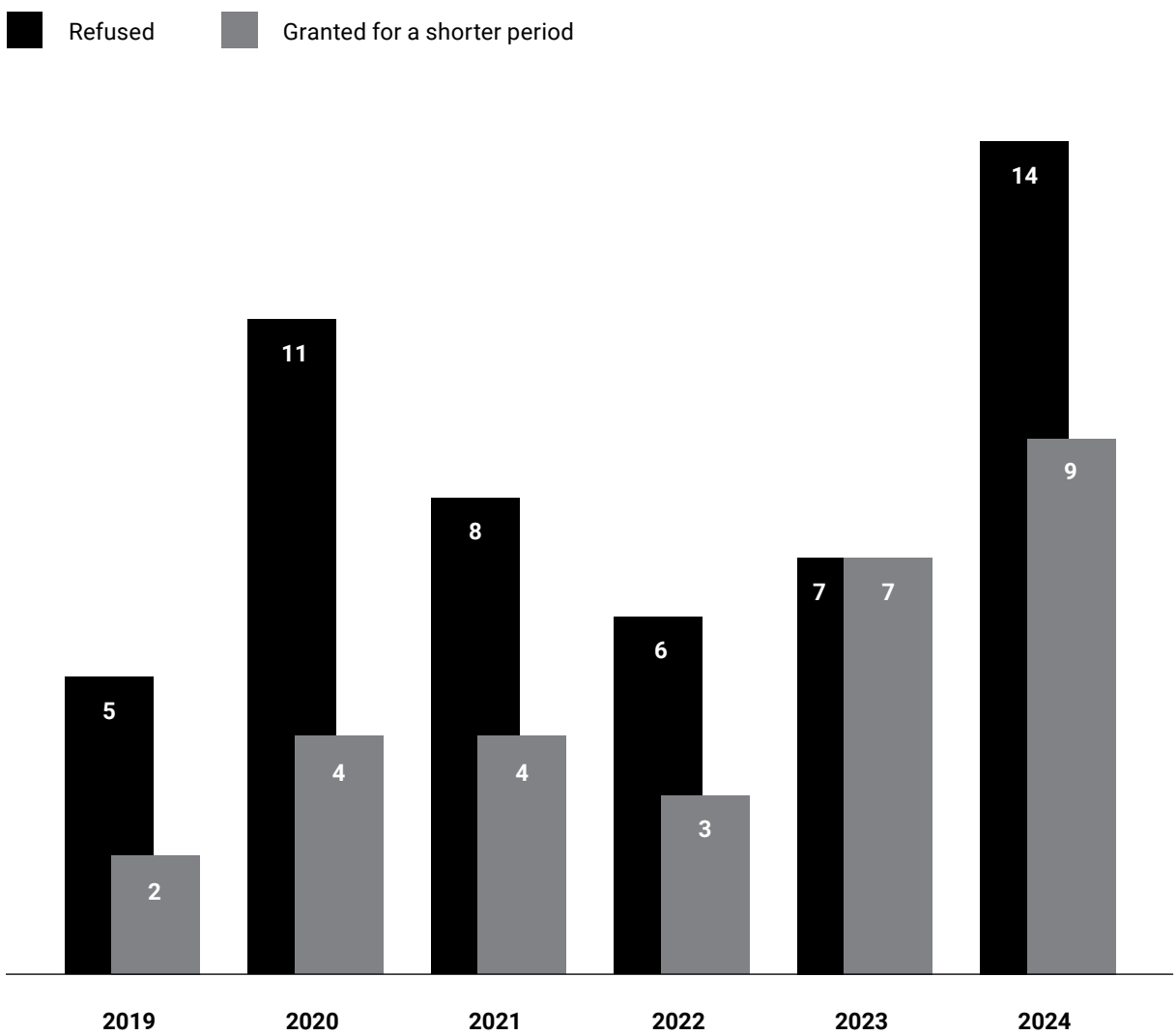
Medically prescribed treatment is, of course, distinct from recreational drug use, and prescribed medication does not hinder eligibility for clearance. Even if someone is facing difficulties today, they might be able to resolve them and successfully complete the vetting process later. Seeking help from a psychologist or psychiatrist should not be seen as a weakness – it shows a willingness to address the issue. If you have a toothache, you see a dentist. If you are struggling emotionally and take steps to deal with it, that is a good thing.

What do you expect from an interviewee?

The most important thing is to be honest and upfront – do not try to hide anything or assume we will not find out. Attempting to deceive us could lead to a refusal. I would advise coming with a positive attitude and an open mind – think of it as an interesting experience. Security clearance is not permanent, and we will meet again when it is time for renewal.

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

The high number of refusals in 2024 was primarily due to issues related to drug use and habitual behaviours that led to a loss of financial independence, such as due to debts or loans.



CYBERSECURITY

Cyber intelligence units are continually evolving, persistently seeking access to Estonia's public and private sector networks.

Emerging trends indicate an increasing use of botnets, or networks of compromised devices, to facilitate man-in-the-middle attacks.

Over the past year, nations hostile to the West have intensified their cyber activities. Both established and emerging cyber threats – entities engaged in cyber espionage – are constantly evolving, relentlessly attempting to infiltrate Estonia's government and private-sector networks.

Cybersecurity is one of the least visible aspects of KAPO's work to protect Estonia's national security. Unlike high-profile cases involving handcuffed spies, corrupt officials on trial or defused explosive devices, cybersecurity rarely makes headlines. The perpetrators of cybercrimes and cyber espionage typically remain anonymous. Hostile cyber activity transcends borders, and even when targeted against a specific country, it rarely affects just one nation. Russian intelligence and influence operations function like a well-oiled machine, with cyber operations serving as both a key instrument and a reinforcing component of its broader strategy.

In 2024, in cooperation with Estonian and international agencies, we publicly identified, for the first time, the perpetrator behind cyberattacks targeting Estonia – an actor operating on behalf of hostile intelligence services.

GRU Unit 29155 had already gained notoriety for its sabotage operations – both physical and cyber operations – long before its involvement in cyberattacks was publicly exposed. As part of the joint attribution effort on 5 September 2024, the United States indicted five GRU officers from Unit 29155, including the previously mentioned Yuri Denisov and Nikolai Korchagin, for their role in destructive cyberattacks against Ukrainian government networks and critical infrastructure in January 2022. These attacks, known as WhisperGate, targeted non-military networks with the aim of spreading chaos, inciting panic among the population, and undermining confidence in the state's ability to secure its systems and data. The ultimate objective was to create conditions that would give Russia a strategic advantage ahead of its planned invasion of Ukraine.

Yuri Denisov

Nikolai Korchagin

Vitaly Shevchnenko

Source: Police and Border Guard Board

On 5 September 2024, Estonia, along with numerous other countries, attributed the 2020 cyberattacks against Estonian government institutions to the Russian military intelligence service, GRU, specifically its Unit No 29155. In Estonia, these attacks, which occurred in November of that year, primarily targeted three ministries: the Ministry of Economic Affairs and Communications, the Ministry of Foreign Affairs, and the Ministry of Social Affairs. Although the attackers failed to obtain any classified information or penetrate critical government networks, they managed to exfiltrate a substantial volume of data, including 350 GB from the Ministry of Economic Affairs and Communications alone.

Although no classified data was compromised, any unauthorised access to information – whether for intelligence gathering, collecting personal data, leaking sensitive materials to discredit the government or individuals, sabotaging state systems or, as seen in Ukraine, erasing critical systems – constitutes an attempt to destabilise a state, instil fear, and sow panic in society. These attacks seek to undermine public confidence in the government's ability to secure its systems and data. This is a non-military assault by one state against another.

A total of 14 partner intelligence services from ten countries collaborated in a joint operation, Toy Soldier, which led to Estonia's public identification of three GRU officers involved in cyberattacks against Estonia on 5 September 2024: Yuri Denisov, Nikolai Korchagin and Vitaly Shevchenko. Following this revelation, the Harju County Court issued arrest warrants for them in absentia. The international investigation also confirmed that additional individuals were involved in cyberattacks targeting multiple EU and NATO countries. These were meticulously planned, state-sponsored operations.

https://rewardsforjustice.net/rewards/foreign-malicious-cyber-activity-against-u-s-critical-infrastructure

The United States has offered a $10 million reward for information leading to the capture of several individuals.

Unlike ordinary cybercriminals, who may abandon an attack if it proves too difficult or costly, state-sponsored operatives are undeterred by setbacks. Intelligence officers and their close collaborators, funded by hostile states, do not have the option to quit – even if an operation is expensive or complex – because they are carrying out their duty. For them, the outcome matters more than the cost. These missions are not motivated by financial gain but by state interests.

Over the past year, all three of Russia's main intelligence services – the GRU, the FSB and the SVR – have continued their efforts to infiltrate Estonia's government networks, both directly and through attacks on partner organisations.

The public disclosure of this case in 2024 will hopefully raise awareness of the threats posed by state-sponsored cyberattacks and accelerate the implementation of necessary security measures.

Hostile cyber actors understand that identifying the source of an attack is crucial for implementing countermeasures. The challenge of attribution remains one of the primary advantages cyberattacks offer their perpetrators. While attributing an attack may not yield immediate or visible deterrent effects, it sends a clear message to adversaries: they cannot operate with impunity. They will be identified, and their actions will provoke a response.

Cyber threats linked to Chinese intelligence services have also intensified. In our previous annual review, we drew attention to the use of botnets in hostile cyber operations, which allow attackers to conceal and obfuscate their activities. Over the past year, we have seen a rise in botnet activity; their use has increased particularly among state-backed Chinese actors, though other cyber adversaries have also employed this tactic.

Botnets are often built using poorly secured internet-connected devices such as routers and other common household gadgets. These devices are frequently outdated, run unpatched software or firmware, retain factory-default settings, or are simply forgotten by users after installation.

Botnets created by cybercriminals and state-backed actors can consist of thousands of compromised devices, making it extremely difficult to trace attackers. This underscores the urgent need for robust cybersecurity measures, not only within government networks but also across personal and private-sector devices. As a nation, we must not expose ourselves to unnecessary risks by neglecting data security.

Just as the number of arrested spies does not fully capture the scale of hostile intelligence activity against Estonia, the true extent of cyber threats against Estonia cannot be measured solely by the number of detected attacks. This is why we once again stress the importance of implementing reliable security measures and promptly addressing vulnerabilities.

Data is a valuable asset

The modern world is driven by data, and our daily lives depend on digital information. It is crucial to recognise that data, particularly personal data, is a valuable commodity. Cybercriminals and state-sponsored cyber espionage actors both seek to acquire data, though their motives differ: criminals seek financial gain, while state actors pursue national interests.

Governments must recognise the value of their data and make sure it is handled responsibly. The state has a heightened duty of care in protecting its citizens' information.

State-sponsored attackers' capabilities continue to grow

The number of state-sponsored cyberattacks is expected to increase as more nations develop their offensive cyber capabilities. These attacks provide a cost-effective and deniable method for intelligence gathering and carrying out influence operations. Beyond targeting government agencies, they may also strike private-sector infrastructure, aiming to disrupt the economy or sow confusion within society.

Network-connected devices can become a weapon for attackers

While humans remain the primary target of cyberattacks, network devices and their security vulnerabilities are increasingly being exploited as attack vectors. This underscores the need for strong patch management, the avoidance of outdated IT systems, and rapid responses to zero-day vulnerabilities through timely identification, patching and mitigation.

Recent trends suggest that botnets and networks of compromised devices will be used more frequently as intermediaries in cyberattacks. This tactic further obscures the attackers' identities, making attribution even more challenging.

Supply chains can be attacked through the weakest link

Given the interconnected nature of modern systems, attacks on supply chains and third-party service providers are expected to become more frequent. A successful breach of a single vulnerable provider can grant attackers access to multiple organisations at once. Cyber adversaries constantly search for weak links in networks and exploit any security gaps they find, which highlights the need for cybersecurity measures across all system components, including external service providers. Close cooperation between the private sector and the state is therefore essential to strengthening cybersecurity and mitigating these threats effectively.

Cloud services introduce new risks

As cloud services see wider adoption, attacks targeting them are also increasing. Misconfigurations, lack of visibility and weak access controls can expose sensitive information to unauthorised parties. To mitigate these risks, organisations must strengthen cloud security configurations, implement zero-trust models and ensure proper encryption of stored data. Users must also maintain oversight of their security solutions and implement robust logging mechanisms to monitor activity within cloud environments effectively.

The growing role of artificial intelligence

The use of artificial intelligence (AI) is playing an increasingly prominent role in influence operations, surpassing its use in traditional cyber espionage. However, attacks aimed at disrupting elections or other democratic processes – such as manipulating public opinion through disinformation – are expected to become more sophisticated and widespread. AI is expected to play an increasing role in such operations – for example, by enabling deepfake technologies that generate highly convincing but inauthentic videos or audio recordings, which can be used to create and spread disinformation.

Preventing cyber threats saves costs

The field of cybersecurity is advancing rapidly as technological advancements and cyber threats become more complex and widespread. Attackers refine their skills and tools, making cyber threats ever more sophisticated. As a result, the importance of cybersecurity in ensuring the smooth functioning of society has never been more critical.

IT security is often perceived as costly, but this is not necessarily the case. Many essential security measures, such as software updates and patching, can be implemented at no expense. Keeping systems up to date and promptly applying patches is one of the most effective ways to mitigate security vulnerabilities. Unpatched systems are among the most common attack vectors exploited by hostile states and cybercriminals.

The vigilance of IT personnel is equally crucial. Carelessness or indifference – whether from an IT specialist or an organisation's leadership – can lead to losses amounting to millions.

Hardware alone holds little value if it is not maintained by skilled professionals who understand how to secure and utilise it effectively. The actual value of technology lies in the expertise and diligence of the administrators and users alike.

In the event of a cyber incident, report it immediately to the Estonian Information System Authority (Riigi Infosüsteemi Amet, RIA), the National Criminal Police (Keskkriminaalpolitsei, KKP) or the Estonian Internal Security Service (KAPO). You never know who might be behind a cyber incident. Given the complexity of tracking cybercriminals, public cooperation and vigilance are essential.

PREVENTING AND COUNTERING EXTREMISM

Extremism is not confined by national borders or age groups.

Efforts to divert individuals from extremism should start as early as possible.

Estonia upholds freedom of expression, thought and action. Constructive dialogue and debate are essential for a functioning and evolving society. Violence, however, has no place in Estonia, and KAPO works to ensure public safety by countering violent extremism.
Extremist and terrorist organisations seek to influence their audience by crafting compelling narratives. By portraying their followers as victims and instilling a sense of duty to resist, they reinforce the belief that their group must be defended and their ideology imposed on others. When violence is framed as the primary solution, individuals influenced by this messaging may be driven to advance terrorist objectives.

Extremism, regardless of ideology, exploits the advantages of an increasingly digital world. Social media, in particular, poses a risk of distorting events through biased or false information. With the internet accessible to all – regardless of national borders or age groups – the transition from online activity to real-world action can occur rapidly, often with serious consequences.

Although the threat posed by violent extremist ideologies remains low in Estonia, sustaining this level requires significant efforts from KAPO. In 2024, we intervened in multiple cases, working not only with adults but also with minors and their parents to prevent acts of violence.

Extremist movements and terrorist organisations exploit young people's digital literacy and the accessibility of social media platforms to spread their ideology. Many young users lack the necessary contextual understanding and critical thinking skills to assess the content they encounter. As frequent consumers of social media, they may become desensitised to violent imagery over time. While their initial exposure to extremist propaganda may not immediately sway them, algorithms amplify the risk by continuously promoting similar content, creating a gradual process of radicalisation. Influencers with large followings play a key role in this process. These figures use public platforms to dictate what is "right" and "permissible" in the interaction between Islam and secular life or to promote ideals of the "true believer" and the "true warrior". Through this type of messaging, audiences are subtly steered towards an extremist worldview.

Young people who fall into the trap of extremism are often searching for a place in society, as well as a means of self-expression, validation and belonging. Their vulnerabilities often stem from social factors, highlighting the need for cooperation between social institutions, communities and support networks to address these risks effectively.

Efforts to divert individuals from extremism should start as early as possible; KAPO intervenes after individuals have already radicalised and their actions may pose a threat to themselves or others.

Far-right extremism

In 2025, the Harju County Court convicted three teenage boys for belonging to the Feuerkrieg Division (FKD), a terrorist organisation that promotes Siege Culture. Groups adhering to this ideology seek to accelerate the collapse of the capitalist system to establish a society they believe aligns with white supremacist ideals. Siege Culture advocates so-called "lone wolf terrorism", urging individuals to take up arms and commit terrorist attacks intended to instil widespread fear and destabilise society. The ultimate objective is to provoke a race war, triggering the apocalyptic collapse of society and its violent reorganisation in favour of white communities.

What makes FKD particularly dangerous is its systematic incitement to terrorism. Members who fight against "racial enemies" are regarded as soldiers, while those who sacrifice themselves in terrorist attacks are glorified as martyrs.

Source: FKD

Given the threat posed by this terrorist organisation – its attempts to recruit members among radicalised minors in Estonia, its access to weapons and ongoing discussions about carrying out attacks – KAPO intervened decisively in the early stages of the terrorist group's formation. The Harju County Court's guilty verdict in January 2025 reaffirmed KAPO's assessment that FKD is a terrorist organisation. The international nature of the threat was further underscored by evidence gathered during the criminal proceedings, which also contributed to countering extremism in other countries.

From a fascination with history to a planned attack

In one case, a minor used a social media platform to threaten an attack on a synagogue. The middle school student had initially developed an interest in National Socialism and topics related to Adolf Hitler. His parents dismissed it as a mere fascination with history. While his classmates also found Hitler-related themes intriguing, their interest remained superficial.

At the same time, the boy described himself as being addicted to social media. On TikTok, he posted content related to monkeys, after which someone in the comments sent him a link to a National Socialist Telegram group. This introduced him to an echo chamber of extremist ideology, where he was exposed to links and other chats featuring violent content. As his radicalisation deepened, he became increasingly interested in the New Zealand mosque shooter Brenton Tarrant and watched videos related

to his attack. He also viewed footage about Anders Breivik, the 2011 mass shooter and bomber in Norway, not realising at first that it was Breivik until this was brought to his attention during a conversation with KAPO. Repeated exposure to extremist content gradually normalised violent rhetoric for him. However, as his radicalisation went unnoticed, the adults around him saw no reason for concern.

At one point, the boy posted in a Telegram group that he wanted to carry out a terrorist attack in Estonia. In response, he was then added to other groups that provided instructions on how to execute such an attack. Within these groups, he specified that he intended to attack a synagogue and even set a date for the assault.

This information reached KAPO, which intervened immediately, conducting a conversation to assess and prevent the threat. While it became evident that the boy was in the process of radicalisation, there was no evidence of concrete planning or active preparation at that time.

Recognise the signs of radicalisation and take action early. Whether you are a parent, teacher, coach or concerned bystander, help young people understand that violence is never a solution. Inform other responsible adults – parents, teachers, coaches – so that the young person can be steered away from a path of violence. If a child is at risk, report it to the local government authority or contact the Child Helpline at 116 111.

Estonia is drafting a deradicalisation action plan

Jana Laht-Ventmann, Consultant at the Department for Juvenile Crimes and Domestic Violence, Estonian Prosecutor's Office

When dealing with radicalised minors, the Prosecutor's Office prioritises intervention measures over punishment, as intervention is more effective in rehabilitating young people and ensuring public safety.

Punishment can exacerbate young people's sense of alienation, increasing the risk that they might return to extremist influences. Needs-driven intervention strategies – such as counselling, educational support or psychological assistance, community programmes, and rehabilitation services can help prevent radicalisation.

Prevention is not only effective for rehabilitating individuals but also plays a broader role in strengthening social cohesion and ensuring long-term security.

Heidi Maiberg, Adviser at the Ministry of the Interior

The Estonian state is developing an intervention model as part of an action plan for preventing radicalisation. The model is designed to support the disengagement and deradicalisation of individuals involved in extremism.

Change cannot be imposed by force. Effective intervention requires the individual's willingness to cooperate and significant societal resources. Therefore, the most cost-effective and impactful strategy is to prevent radicalisation before it takes hold. A key objective of the new action plan, led by the Ministry of the Interior, is to develop training materials and guidelines to help professionals working with young people recognise signs of extremism and, through their everyday work, contribute to its prevention.

Kremlin-backed right-wing extremism

Russia exploits even the smallest societal vulnerabilities to conduct hybrid attacks. Over the past year, our counter-extremism efforts have prioritised preventing such attacks orchestrated by the Russian Federation. As part of these preventive measures, Estonia has revoked residence permits on security grounds for individuals deemed at serious risk of being exploited in support of Russia's military objectives.

In January 2025, on KAPO's recommendation, Estonia revoked the residence permits of two stateless individuals linked to the paramilitary wing of the Russian Imperial Movement, known as the Russian Imperial Legion, and its training centre, Partizan. The United States and Canada have designated the Russian Imperial Movement as a terrorist-supporting organisation, and the European Union has imposed sanctions on the group due to its paramilitary wing's participation in Russia's war of aggression in Ukraine, including involvement in war crimes in Bakhmut.

Before revoking the residence permit, KAPO attempted to mitigate the immediate threat by engaging in a preventive discussion with an individual linked to the movement. However, the person chose to leave for Russia, where they continued collaborating with the Russian Imperial Legion. Given the persistent security risk, revoking this individual's residence permit became the only viable option to counter the threat posed by Russia's hybrid attacks and terrorism.

Estonia has seen an increase in vigilante-style attacks inspired by Russian far-right ideologue Maxim Martsinkevich, also known as Tesak. One particularly concerning trend is the emergence of so-called "paedophile hunting" operations, where individuals take extrajudicial action against others using violent methods.

In 2024, an attempt was made to establish a Russian-language far-right Telegram channel in Estonia under the name NS/SK!HOB. The channel spread violent extremist and terrorist propaganda and sought to organise acts of violence within the country. While the channel attracted several thousand followers, only a handful had ties to Estonia – the majority were based in Russia. KAPO identified a minor in Estonia who was the channel's administrator. After warning the individual and their parents

Source: Estonian Internal Security Service

Russian citizens have attempted to infiltrate far-right organisations in Estonia to undermine the cohesion of Estonian society.
Source: Estonian Internal Security Service

about the possible consequences, we worked with them to shut down the channel. This intervention helped prevent the further spread of Russian hybrid influence, far-right violence and terrorist propaganda in Estonia.

Among the followers of this Telegram channel were also members of Active Club Estonia, a group mainly engaged in promoting Tesak-style vigilante operations in Estonia. In 2024, three Active Club Estonia members were convicted for their involvement in such activities. One of the group's members also administered the Telegram channel "Pedo Hunting Estonia".

That same year, Active Club recruited a Russian national who had left Russia and publicly presented himself as a supporter of Ukraine and the Azov Regiment. In reality, he was aiding Russian propaganda efforts by attempting to link support for Ukraine – and, by extension, its adversary Azov – with far-right extremism and neo-Nazism. To prevent Russian nationals from undermining Estonia's social cohesion, this individual's residence permit was revoked, a deportation order was issued, and he was banned from re-entering the country.

Islamic extremism

Although Estonia's Muslim community has historically been peaceful, some previously moderate community members have recently shown signs of radicalisation due to external influences, including exposure to terrorist propaganda.[25] A key trigger in 2024 was the conflict between Israel and the Hamas terrorist organisation, which led to an increase in anti-Semitic sentiment. In response, Estonian authorities revoked the e-residency status of four individuals, cancelled one residence permit and imposed an entry ban on another individual.

Terrorist organisations exploit issues that resonate with Muslim communities to fuel radicalisation and incite conflict. Narratives of Muslim oppression and alleged attacks on Islam are commonly used as tools of influence. Daesh and al-Qaeda, for example, framed Hamas' assault on Israel as part of a global jihad. They used the attack to mobilise their supporters, even though they had not previously regarded Hamas – an Iranian-backed organisation with regional objectives – as part of a broader global jihadist movement.

The spread of extremist ideology relies on expanding its support base, which is often fuelled by societal polarisation that creates divisions. These divisions can be based on profound ideological differences or can revolve around specific issues. After the Hamas attack in October 2023, Islamist propaganda shifted its narrative to portray Jews and Israel as the primary adversaries rather than focusing solely on Western countries and Western influence. However, Western nations still remain on their list of adversaries.

Extensive propaganda efforts continue to focus on Hamas, Hezbollah and the Israel conflict. In last year's annual review, we highlighted Hamas' intensified efforts to spread its narrative. In Estonia, individuals supporting Hamas' narrative have expressed their views peacefully, thanks in part to continuous preventive efforts. Unlike in the United States and parts of Europe, where protests have disrupted university operations, such activities have not escalated in Estonia – although calls for such actions have been made.

In 2024, authorities were compelled to intervene in the case of a schoolboy who had been radicalised, primarily through online platforms. His interactions with like-minded individuals and consumption of extremist material led to ideological clashes at school and, ultimately, a desire to carry out a terrorist attack in Estonia.

The Muslim community in Estonia

Traditionally peaceful, the Muslim community in Estonia continues to grow, primarily due to immigration. With approximately 10,000 members from diverse national backgrounds, events in their home countries inevitably influence their lives in Estonia. The main obstacles to integration remain language barriers and the tendency to limit social connections primarily to the local Muslim community.

The year 2024 brought significant changes for Estonia's Muslim community. The long-standing imam stepped down from his role due to conflicts with other community members, his ties with Russian Islamic leaders,[26] his promotion of Hamas narratives and actions driven by personal gain. These factors left no alternative but his departure.

KAPO also identified a foreign imam as a security risk to Estonia. His activities – driven largely by personal gain – were aimed at dividing the Estonian Muslim community and fuelling internal conflicts.

As communities grow, they gain greater autonomy, creating opportunities for ambitious individuals to seek leadership roles. This, in turn, increases the influence of external actors in Estonia and may attract more followers to different religious doctrines.

Shia Muslims in Estonia

In 2024, the conflict between Israel and Hamas,[27] and Hezbollah[28] had global repercussions. In Estonia, issues related to imams and the growth of the Muslim community have contributed to the emergence of a distinct Shia[29] religious movement. Previously, the Estonian Islamic Centre represented all Islamic denominations, but its role has diminished as Shia Muslims have begun establishing an independent religious presence in the country.

Within this newly established movement, events featuring guest imams from abroad and online religious services have been organised. Some of these invited speakers have previously expressed support for Hezbollah's leader on social media. In 2024, efforts were made to officially register a Shia religious association in Estonia. Although many Shia Muslims in Estonia have lived, studied and worked in the country for years, they continue to be influenced by global developments. They have made social media posts praising Hezbollah's former leader, Hassan Nasrallah,[30] as a martyr and glorifying Iran's Supreme Leader Ali Khamenei for orchestrating attacks on Israel. Plans were also made to hold a gathering to commemorate Nasrallah's so-called martyrdom. KAPO has observed a rise in anti-Israel and anti-Jewish sentiment among Estonia's Shia community.[31]

25 See also the chapter "Preventing and countering international terrorism".
26 Like Patriarch Kirill of Moscow, the Grand Mufti of Russia and regional muftis have declared the war in Ukraine a holy war. The Estonian Shia community mainly consists of Pakistani and Indian nationals.
27 Hamas is a Palestinian nationalist Sunni Islamist political organisation that the United States and European Union have designated as a terrorist organisation.
28 Hezbollah is a Lebanese Shia Islamist party and paramilitary group that the United States and European Union have designated as a terrorist organisation.
29 The Estonian Shia community mainly consists of Pakistani and Indian nationals.
30 The leader of Lebanon's Shia Islamist Hezbollah movement, who was killed in September 2024.
31 Iran's supreme leader and the Iranian Revolutionary Guard Corps (IRGC) promote Mahdism, which identifies Israel as the main enemy of the Shia.

PREVENTING AND COUNTERING INTERNATIONAL TERRORISM

Terrorist propaganda is increasingly targeting minors; new legislation in Estonia enables more effective intervention.

Funds collected under the guise of humanitarian aid for conflict zones may be misappropriated to finance terrorism.

Terrorist organisations such as al-Qaeda and Daesh (also known as the Islamic State or ISIS), along with their affiliated groups, are expanding their influence in Africa and Central Asia. They also continue to maintain strongholds in the Middle East. Islamist terrorism remains one of the primary non-military threats to European states.

Islamist terrorist organisations use existing conflict zones to expand their operational reach; they also instigate conflicts. The main areas of Islamist terrorism today are sub-Saharan Africa and Afghanistan. In the Middle East, Islamist terrorism has been significantly weakened. In Syria, the effectiveness of counter-terrorism efforts will depend on the new regime's ability and willingness to maintain stability and security in the country.

Afghanistan is currently regarded as a safe haven for terrorist organisations, allowing them to operate with minimal external interference, aside from the ongoing conflict between Daesh and the Taliban regime. The Khorasan Province branch of Daesh (Islamic State Khorasan Province, ISKP) has regained its capacity to support external operations, making the identification and dismantling of its networks in Europe a key priority for security agencies.

Although external operations remain challenging and resource-intensive, terrorist organisations are encouraging their supporters who already live in Europe to carry out attacks.

While the terrorist threat level in Europe remains high, Estonia continues to face a relatively low level of risk. However, we are observing a growing number of individuals with ties to terrorism establishing connections in Estonia. Through preventive measures, we have successfully prevented such individuals from settling in the country.

In Europe, the terrorist threat is primarily driven by the activities of organised networks and individuals with direct links to terrorism who exploit the Schengen visa-free travel system. Focused efforts by security agencies have hindered the expansion of these networks. These efforts have been bolstered through effective identification measures and international cooperation. However, restrictions on data sharing between countries remain a significant obstacle

to detecting terrorists. Each country maintains its own databases, which are inaccessible to other states. As a result, changes in identity, residence permits and asylum application records may go unnoticed, allowing terrorists to conceal their identities and evade detection.

Case study

An individual with terrorist ties attempted to start a business in Estonia

- Individual X, of European origin, travels from Europe to Syria in year Y and joins a terrorist organisation.
- X spends several years in Syria, directly participating in terrorist activities.
- After several years, X returns to Europe from Syria.
- X legally changes their name in their country of residence.
- Under their new identity, X applies for an Estonian e-residency to establish a business. Due to the name change, their previous terrorist affiliations go undetected.
- After obtaining e-residency, X sets up a company in Estonia; however, the business does not engage in any economic activity within the country.
- X visits Estonia on several occasions, including visits to a shooting range, where they practise using various firearms.
- KAPO determines that X exploited a name change to obtain e-residency undetected.
- Based on KAPO's recommendation, Estonia imposes a 10-year entry ban on X.
- As the entry ban takes effect while X is in Estonia, the Police and Border Guard Board detains and deports X.

Battlefield and information warfare

Terrorist organisations regard propaganda efforts as crucial as carrying out attacks. Daesh has explicitly stated this priority, stating that its soldiers fight on two fronts – the battlefield and the war of words. Terrorist propaganda is designed to be concise, striking and optimised mainly for social media engagement. It is translated into multiple languages to reach the broadest possible audience. Dissemination efforts are driven by individuals who actively spread propaganda on behalf of terrorist groups. While public social media channels serve as a tool to spark initial interest, the process of radicalisation typically unfolds on more covert platforms that prioritise anonymity. An increasing number of young people, including minors, are gaining access to extremist propaganda.

Several terrorist attacks in the EU have been planned and carried out by minors. This trend is partly due to the challenges in assessing their level of radicalisation and attack risk, particularly when much of their interaction takes place in online environments that either ensure anonymity or refuse to cooperate with law enforcement. Striking the right balance between overreaction and proactive intervention remains a key challenge in countering Islamist extremism.

Terrorist propaganda is spread through major platforms such as Meta, Instagram, TikTok and Discord, but ideological influence and recruitment take place on anonymity-preserving platforms such as Telegram, Element, Threema, Sessions and Conversations.

Artificial intelligence is now being used to generate and translate propaganda into multiple languages, which makes extremist content more accessible than ever before.

Legislative amendment to restrict terrorist propaganda

On 14 July 2024, amendments to the Information Society Services Act came into force, aligning Estonian legislation with the European Union regulation on addressing the dissemination of terrorist content online, known as the Terrorist Content Online (TCO) Regulation. Terrorist online content is considered a major catalyst for radicalisation; it incites or solicits individuals to commit terrorist acts or contribute to their execution. It may also solicit individuals to participate in the activities of a terrorist group.

Terrorist propaganda glorifies terrorist activities, disseminates materials depicting terrorist attacks and provides instructions for the production or use of explosives, weapons, and chemical, biological, radiological or nuclear (CBRN) substances. Terrorist online content includes text, images, audio recordings and videos, as well as live broadcasts of terrorist acts, which pose an ongoing risk of further such offences being committed.

These propaganda channels enable terrorist organisations to:

- **Increase their visibility**
- **Spread fear**
- **Influence Muslim communities in Europe by amplifying false narratives of discrimination**
- **Expand their supporter base**
- **Recruit new members**
- **Incite attacks**
- **Provide guidance on planning attacks and making explosives, poisons and weapons**

In 2024, Estonia recorded a sharp rise in visits by individuals with links to Islamist terrorism, identifying over 214 such cases. Previously, an average of 50 such individuals visited Estonia annually. Since the outbreak of the war in Ukraine, the number of high-risk individuals exploiting Schengen travel freedoms has doubled. Additionally, the closure of the Finland-Russia border further contributed to the surge in such cases in Estonia in 2024.

An exception is made for material disseminated for educational, journalistic, artistic or research purposes to prevent or counter terrorism.

In Estonia, KAPO is responsible for monitoring the dissemination of terrorist content, verifying such messages and issuing orders to remove material. Since the legislative amendment came into force in 2024, KAPO has issued multiple removal orders for terrorist online content. We urge the public to report any suspected terrorist propaganda found online, including on social media platforms. Reports can be submitted via email at tco@kapo.ee or by calling us at +372 612 1455. More information is available on our website at www.kapo.ee.

Hamas propaganda aims to shift the focus from Hamas' actions in the Gaza conflict to broader support for Palestine. Source: ERR

Terrorist financing

The sources of terrorist financing in Europe remain largely unchanged, with funds generated through business revenues, organised crime, regular donations and crowdfunding campaigns. However, there is a growing reliance on modern cross-border payment services to finance terrorism. At the same time, traditional cash couriers operating within the *hawala* network[32] also remain in use for illicit financial transactions.

Estonian credit institutions are well aware of the risks associated with terrorist financing. However, offering services through VIBAN accounts, commonly linked to international payment service providers and virtual currency platforms, continues to present a security risk. Close cooperation between credit institutions and the public sector remains essential for mitigating these threats.

In 2024, the highest-risk transactions related to terrorist financing were those linked to the Gaza region. Given that financial donations have been made from Estonia to individuals in this conflict zone, it is important to note that the same crowdfunding platforms – most notably Patreon and GoFundMe – are also used by individuals and groups with ties to terrorism.

A member of the Muslim Brotherhood also participated in a pro-Palestine protest in Tallinn in 2024, inciting violence. Source: ERR.

The same risks apply to donations made through foreign non-profit organisations (NGOs). In many cases, it is nearly impossible to determine the final recipient of the funds, how much of the donation actually reaches those in need and whether any portion ends up in the hands of individuals linked to terrorism. New foreign NGOs are continually emerging in crowdfunding efforts, often copying the names and social media content of legitimate organisations. Turkey-based NGOs, in particular, have stood out in this regard, making it difficult to distinguish between genuine and fraudulent organisations.

We strongly advise donors to thoroughly research where and to whom they are sending money and how the funds will be used locally. Additionally, it is prudent to verify the recipient's name against available sanctions lists, such as the EU Sanctions Map (www.sanctionsmap.eu) or the Estonian Financial Intelligence Unit (www.fiu.ee).

Virtual assets in terrorist financing

Hamas and Palestinian Islamic Jihad, both listed under European Union sanctions, actively called for financial support in 2024, including through virtual assets. Other major terrorist organisations, such as Daesh and al-Qaeda, employ similar tactics. These schemes often exploit virtual asset service providers (VASPs) that lack licences and do not implement proper due diligence measures, particularly Know Your Customer (KYC) procedures. They also use intermediaries and shell organisations to obscure the ultimate beneficiary of the funds.

The Estonian-licenced VASP sector has largely been cleaned up, with only a few firms reporting transactions suspected of terrorist financing to the Estonian Financial Intelligence Unit. However, despite the common perception that blockchain transactions are

transparent and traceable, this is not always the case. KYC compliance is crucial, and many risks stem from service providers based in third countries that do not enforce KYC regulations. Additionally, tools such as mixing and swapping services and privacy coins are explicitly designed to hinder transaction traceability in the blockchain under the pretext of ensuring user privacy.

Further risks arise from transactions involving international contractual partners. For example, Estonian-licenced VASPs offering nested services – a structure similar to correspondent banking, where a single account may hide hundreds or thousands of sub-clients – pose a significant challenge to effective monitoring. This is particularly problematic when dealing with service providers registered in offshore jurisdictions.

The total annual transaction volume of Estonian-licenced VASPs exceeds €30 billion across various services, with Estonian residents accounting for less than 10% of these transactions. Risks persist among VASPs that maintain correspondent relationships with third countries where due diligence measures are inadequate and where payment options in privacy coins are available. Additionally, anonymous prepaid and gift cards from neighbouring countries are becoming increasingly popular, further complicating oversight.

In 2024, KAPO prevented a European Union citizen with ties to the Kurdistan Workers' Party (Partiya Karkerên Kurdistan, PKK)[33] and Daesh in Syria from establishing a business in Estonia. Additionally, a United Arab Emirates resident who had links to terrorism was blocked from setting up an IT company, which could have been used as a front for financing terrorist activities. Both individuals were issued entry bans to Estonia, and one person's e-residency was revoked.

Since the launch of the Estonian e-residency programme in 2014, 31 foreign nationals with links to Islamist terrorism and extremism have been identified as current or former e-residents or applicants, including three cases in 2024. Furthermore, individuals associated with other forms of extremism and security threats have also been observed among e-residents and applicants.

Illegal handling of firearms and explosives

KAPO focuses on cases of arms trafficking that involve violations of firearm handling requirements during their transport across state borders or pose a threat to Estonia's national security, independence or territorial integrity.

In October 2024, the Police and Border Guard Board, in cooperation with the Rescue Board, conducted a campaign encouraging the voluntary surrender of firearms and explosives to reduce risks to their owners and the public. As part of the campaign, individuals

32 Hawala is a traditional trust-based method of transferring money in Islamic countries, which does not require cash to physically travel to the recipient. Instead of cash, the hawaladar, or broker, may also accept valuables, immovables or movables, which are converted into cash handed over to the recipient.

33 A Kurdish terrorist organisation.

were invited to turn in illegal firearms, ammunition and explosives without fear of prosecution. Over the course of a month, 26 illegal firearms, two essential firearm components, thousands of rounds of ammunition and 423 units of explosive material were surrendered.

A similar threat to explosives is posed by pyrotechnics, which are increasingly being used for criminal purposes worldwide. In Europe, criminals have used pyrotechnic materials for various offences, including ATM robberies. In recent years, there has been a noticeable increase in the illegal import of pyrotechnic products into Estonia.

Additionally, cases involving modified signal weapons converted into functional firearms have also increased. Signal and alarm weapons are freely available in Estonia, allowing any adult to purchase them legally. Depending on the brand and design, converting these weapons into functioning firearms can be relatively simple. Firearms converted from signal weapons purchased in Estonia have been used abroad in serious crimes, including homicides.

Overall, however, the threat of illegal handling of explosives, the use of explosives in attacks and the cross-border smuggling of firearms remains relatively low in Estonia.

Homemade explosive led to severe injury and imprisonment

In early 2024, Lembit Pedak, known as the Käravete bomb maker, came to public attention following a failed attempt to blow up a snowbank with a homemade explosive device concealed inside a toilet paper roll. The device detonated prematurely in his hand, causing serious injuries.

To obtain the precursor chemicals needed to produce the explosive, Pedak misled a chemical company, falsely claiming that he was purchasing the substances for various businesses where he performed small-scale work. Instead, he used them to manufacture TATP (triacetone triperoxide), a highly volatile explosive, which detonated in his hand, severing it.

Pedak's actions endangered not only himself but also his neighbours and their families. The outbuilding where he stored a large quantity of the highly volatile explosive was located near a children's play area. While the toilet paper roll device contained approximately 50 grams of TATP, had the entire stockpile in Pedak's shed exploded, the blast radius would have extended at least 250 metres. Due to the extreme volatility of TATP, the Rescue Board's bomb disposal experts deemed transportation too risky and had to neutralise it on-site.

Since 2014, terrorists have used TATP in six separate attacks across Europe. The three most recent incidents occurred in 2017: an attempted bombing at Parsons Green underground station in London, an explosion at a Brussels railway station and the Manchester Arena attack, in which a suicide bomber detonated a TATP device, killing 22 people and severely injuring more than a thousand.

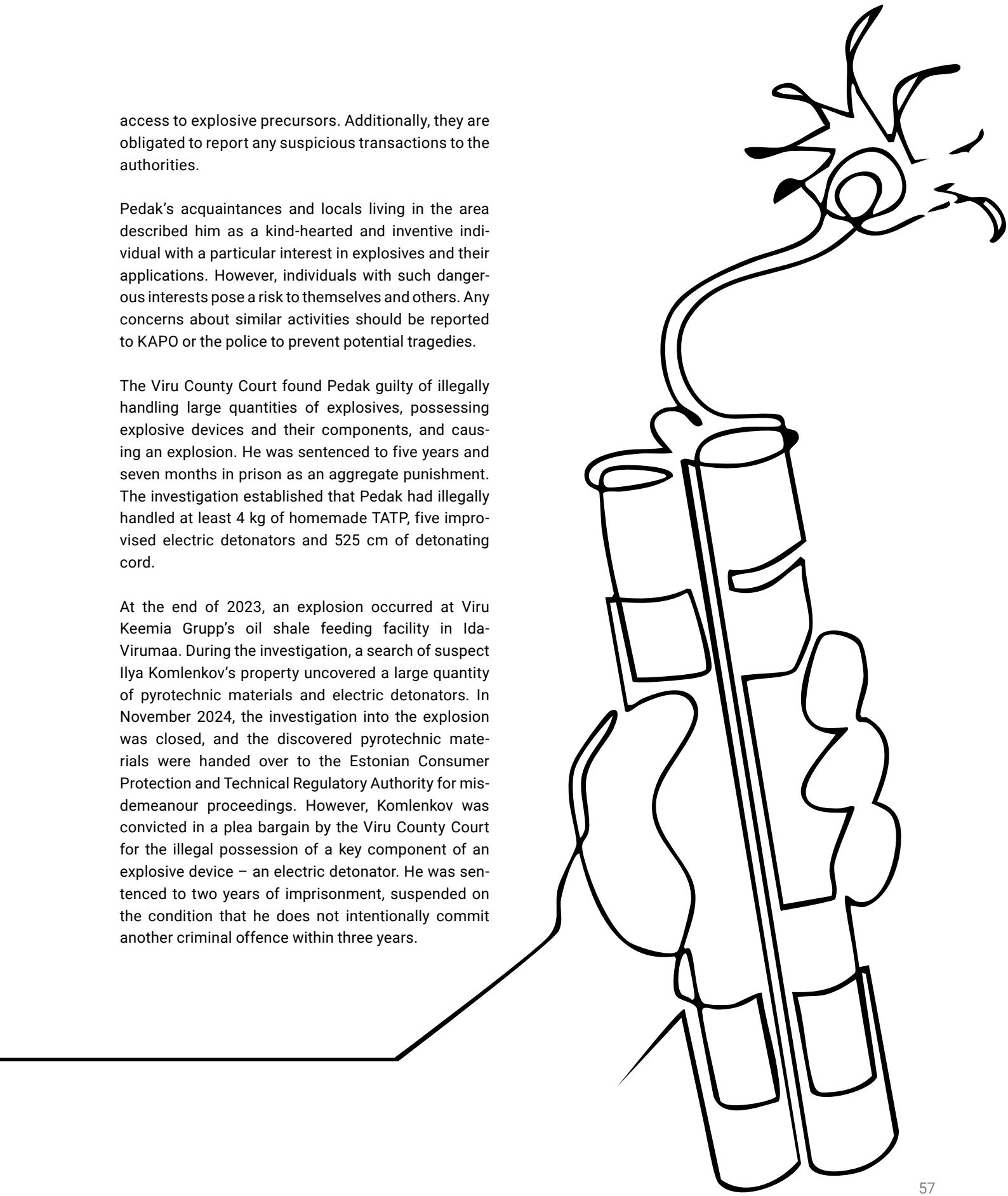
Chemical companies are required to exercise particular caution when selling precursor chemicals for TATP production. They must verify the identity of the purchaser, confirm the intended use of the substances and comply with regulations restricting

access to explosive precursors. Additionally, they are obligated to report any suspicious transactions to the authorities.

Pedak's acquaintances and locals living in the area described him as a kind-hearted and inventive individual with a particular interest in explosives and their applications. However, individuals with such dangerous interests pose a risk to themselves and others. Any concerns about similar activities should be reported to KAPO or the police to prevent potential tragedies.

The Viru County Court found Pedak guilty of illegally handling large quantities of explosives, possessing explosive devices and their components, and causing an explosion. He was sentenced to five years and seven months in prison as an aggregate punishment. The investigation established that Pedak had illegally handled at least 4 kg of homemade TATP, five improvised electric detonators and 525 cm of detonating cord.

At the end of 2023, an explosion occurred at Viru Keemia Grupp's oil shale feeding facility in Ida-Virumaa. During the investigation, a search of suspect Ilya Komlenkov's property uncovered a large quantity of pyrotechnic materials and electric detonators. In November 2024, the investigation into the explosion was closed, and the discovered pyrotechnic materials were handed over to the Estonian Consumer Protection and Technical Regulatory Authority for misdemeanour proceedings. However, Komlenkov was convicted in a plea bargain by the Viru County Court for the illegal possession of a key component of an explosive device – an electric detonator. He was sentenced to two years of imprisonment, suspended on the condition that he does not intentionally commit another criminal offence within three years.



CBRN: chemical, biological, radiological and nuclear weapons

In 2024, Russia deployed chemical weapons on the battlefield on more than 400 occasions. Since the full-scale invasion began in February 2022, Ukrainian intelligence has recorded more than 5,000 incidents of Russian forces using hazardous chemicals along the front lines.

The Ukrainian Ministry of Defence has repeatedly reported that Russia has employed tear gas and other chemical irritants in combat – substances that are banned for military use under the Geneva Convention. Additionally, white phosphorus has also been widely used, particularly in the Donetsk and Zaporizhzhia regions. While not classified as a chemical weapon, white phosphorus causes severe burns, and its use against civilians constitutes a war crime.

Russia has repeatedly attacked Zaporizhzhia, Europe's largest nuclear power plant, turning it into a potential radiological disaster source.

CBRN threats – encompassing chemical, biological, radiological and nuclear weapons – are not confined to the security concerns of a single nation. These weapons serve as strategic offensive tools, posing a serious risk to Europe and the entire world.

In recent years, there have been multiple confirmed cases of CBRN weapons use globally. Some of these may be part of broader strategic attacks, while others likely remain unresolved due to a lack of awareness or expertise.

States have also used CBRN agents to eliminate political opponents. In 2018, the nerve agent Novichok was used in the UK against former Russian military intelligence officer Sergei Skripal and his daughter Yulia. In 2020, Russian opposition leader Alexei Navalny was poisoned with the same nerve agent. Such use of chemical weapons as a tool of political coercion often goes unpunished.

There is also a growing risk in Europe that terrorist organisations may seek to acquire knowledge and disseminate skills on how to use CBRN agents effectively and with readily available materials.

Preventing and countering CBRN threats, as well as responding to incidents, requires expertise, rapid response capabilities and strong cooperation at the international and national levels. This includes restricting the spread of suspicious materials and goods and monitoring the potential misuse of CBRN-related technologies. Preventing panic and providing clear guidance are crucial in both detecting and resolving such crimes. The challenge of CBRN attacks lies in the difficulty of immediately identifying intentional actions.

Although the likelihood of a CBRN attack in Estonia or Europe remains low, examples of attacks elsewhere in the world underscore the importance of preparedness in mitigating potential threats.

Explosion carried out during TATP demining. Source: Rescue Board

ECONOMIC SECURITY

Russia's aggression has demonstrated that energy infrastructure is its primary target for undermining the resilience and morale of its adversaries. Disconnecting the Baltic states' power grid from the Russian frequency area was a historic step, but we must remain committed to achieving full energy independence.

Russia requires strategic goods and is attempting to import them through complex networks and trade routes.

Hostile states are increasingly seeking to expand their foreign investments.

KAPO is responsible for safeguarding the independence of Estonia's economic policy decisions. When significant decisions are made without proper preparation, they can inadvertently sow the seeds of future security challenges. Vulnerabilities often emerge from environments prone to corruption, poorly planned supply chains that create dependencies, or a deteriorating economic and competitive landscape for businesses. When the national economy faces challenges, maintaining security becomes even more difficult.

Due to the interconnected nature of the global economy, we collaborate closely with our allies to safeguard our economic security. As a member of the European Union, and in choosing our more distant partners, we have determined which dependencies are acceptable and who our like-minded allies are.

Our values also define what is unacceptable for Estonia. Establishing economic ties with an expansionist and aggressive Russia is not an option, nor is developing a dependence on an authoritarian China with global ambitions. In our economic relations with China, it is crucial to assess long-term consequences by recognising our vulnerabilities and dependencies. With Russia, however, there is no ambiguity: its war machine must be stopped.

Russia's capacity to wage war is closely linked to its economy, making it vulnerable to external pressure. A sanctions policy is designed to exploit this vulnerability.

Sanctions are effective, and we recognise the efforts of our partners who enforce them on the front lines every day. We also commend the media for playing a vital role in exposing businesses that attempt to exploit legal loopholes and encouraging them to realign their moral compass.

Estonia has successfully advocated for several EU sanctions aimed at restricting Russia's access to critical technology and decreasing its energy export revenues. Although more could be done at the EU level, opposition from some member states has made the adoption of additional sanctions increasingly difficult. Exemptions granted to secure consensus weaken sanctions and complicate their enforcement and oversight.

A major challenge with sanctions is Russia's ability to circumvent them through countries that do not align with Western sanctions. Unfortunately, Western products continue to reach Russia through third countries and numerous intermediaries. We encourage those who still consider the situation merely a "temporary inconvenience" to recognise these tactics and reconsider their indirect role in sustaining Russia's war machine through supply chain involvement.

Russia has prioritised the needs of its defence industry by increasing the production of military equipment and munitions while replenishing its stockpiles. The country openly cooperates militarily with strategic allies such as Iran, North Korea and China. Russian procurement is increasingly relying on companies from China, Central Asia and even Turkey. These firms often source goods from European suppliers, where individuals who directly liaise with Russian businesses or are otherwise aware of the goods' actual end-use facilitate these transactions. To obscure the paper trail of documents, various companies – some registered in tax havens – are used for payments, transportation and customs documentation. Although extending procurement chains has enabled Russia to secure the desired goods, the increasing number of intermediaries has made the process more costly and slower.

Strategic goods for the Russian military

Several Estonian companies have been involved in procurement networks that facilitate the transfer of strategic goods from US or European manufacturers to third countries, from where these goods are redirected to Russia's military industry. KAPO gathers intelligence on such companies to assess whether their support in enhancing Russia's military capabilities is intentional. Under current law, individuals found guilty of illegally transporting prohibited strategic goods or providing related services face prison sentences of three to twelve years. If a group commits the offence, the sentence ranges from five to twenty years.

In spring 2023, KAPO launched a criminal investigation into Denis Ignatiev, a Russian citizen residing in Estonia. He was suspected of ordering and facilitating the transport of sanctioned and strategic goods, including scopes, binoculars, and telescopes, to Russia via the Narva border crossing. The investigation revealed that Ignatiev placed orders through

Source: Estonian Internal security Service

online retailers in Poland and other EU countries. The scheme involved multiple individuals: Ignatiev was responsible for ordering, logistics, storage and forwarding the items, while another Russian citizen residing in Estonia, Ruslan Sibilev, managed the payments. Sibilev used bank accounts associated with foreign-registered companies he controlled to process these transactions. The goods were delivered by courier to Ignatiev's home address. The investigation into Ignatiev was eventually closed following his death.

In autumn 2024, Sibilev reached a plea agreement with the Estonian Prosecutor's Office. The court found him guilty of aiding and abetting the violation of international sanctions and providing services related to strategic goods without the required special licence. As a result, he was fined €79,557.50. The authorities also confiscated goods worth €200,000 that were intended for shipment to Russia. Sibilev surrendered these items to KAPO. The confiscated strategic goods, which were initially meant to support Russia's military operations in Ukraine, were instead donated to Ukraine.

In June 2024, Russian citizen Demyan Belyakov was detained while attempting to smuggle restricted strategic goods – firearm suppressors and their components – out of Estonia through the pedestrian terminal at the Narva border crossing. At the checkpoint, Belyakov falsely claimed that the items were water pump parts. A search at his company, Filtronics OÜ, uncovered 44 fully assembled firearm suppressors and more than 5,500 different suppressor components. Belyakov, who also operated a business in Russia, had a signed purchase agreement with a Russian NGO, Kalashnikov Concern Training Centre, under which he was contracted to supply 100 units of sound and flash suppressors. The Viru County Court sentenced him to five years of effective imprisonment under a plea agreement.

Given the current security situation, any effort to make sanctioned or military-use goods accessible to Russia supports its aggression and must be prevented.

Russian shadow fleet vessel Eagle S. Photograph: Scanpix

Energy security

The ongoing conflict has demonstrated that the Russian Federation is deliberately and systematically destroying Ukraine's energy infrastructure to undermine its resilience and morale.

A historic step in strengthening energy security – a cornerstone of economic security – was taken on 8 February 2025, when the Baltic states disconnected from the Russian and Belarusian electricity grid and successfully synchronised with the continental European network. Beyond the immediate efforts of energy companies and those directly responsible for ensuring the transition, a variety of businesses and government agencies prepared for contingencies during this critical process. However, crisis preparedness must remain a priority and continuously rehearsed as the threat of hybrid attacks on infrastructure orchestrated by an aggressor state persists.

Operators of critical infrastructure must strengthen both their physical and digital resilience. Although the Estonian Foreign Ministry has advised against travel to Russia, a significant number of employees at critical service providers continue to visit the Russian Federation regularly. Many of these individuals do not fully understand the risks associated with travelling to and staying in Russia for extended periods.

Alongside its regular responsibilities, KAPO has worked with key service providers to enhance their awareness of critical vulnerabilities. These may include weaknesses related to supply chains, inadequate adherence to security protocols, poor cyber hygiene, or internal threats posed by employees. Organisations concentrating on their core business operations may sometimes overlook evolving risks. We will continue in our preventive efforts to strengthen collective preparedness for potential crises.

Recent incidents of damage to undersea infrastructure in the Baltic Sea are a concerning development. KAPO is currently conducting a criminal investigation into the severed communication cables that occurred in October 2023. At the same time, Finnish authorities are investigating the damage to the Balticconnector gas pipeline the same month. Since then, underwater connections between Latvia, Finland and Sweden have also been damaged. The latest incident involving Estonia occurred in December 2024, concerning the Estlink 2 power cable between Estonia and Finland. Due to the location of the fault, the investigation is led by the Finnish National Bureau of Investigation. Preliminary findings indicate that the incident was caused by the cargo ship Eagle S, which is part of Russia's shadow fleet, dragging its anchor across the seabed.

China and Russia can quickly and cost-effectively destroy subsea communication cables. However, investigations into incidents in the Baltic Sea have yet to produce sufficient evidence to classify them as deliberate sabotage.

Russia's shadow fleet consists of ageing vessels that would typically be decommissioned under normal circumstances. The crews operating these ships often lack experience and proper training and frequently display negligence in their duties. In addition to the potential for infrastructure damage, this fleet also poses a significant environmental risk.

Cargo is the most valuable asset for shadow fleet operators. Past incidents in the Baltic Sea have demonstrated that shipowners often disregard the welfare of their crews.

There is an ongoing risk of damage to undersea cables. All Baltic Sea nations are collaborating to monitor vessel movements and activities, respond swiftly and decisively to incidents, gather evidence of intent, and hold those responsible to account.

Foreign investments

The security risks associated with foreign investments have become an increasing concern for the European Union, including Estonia. States that oppose Estonia's security interests, particularly Russia and China, are seeking to expand their influence by acquiring stakes in strategic enterprises or taking over their key economic activities. In light of recent crises and shifts in global power dynamics, the likelihood of hostile states using their foreign investments to advance their security policy objectives is expected to grow. Such investments could compromise Estonia's security and public order, creating dependencies that leave the country vulnerable to external influence by hostile states.

KAPO is responsible for evaluating foreign investments that may pose security risks to strategic assets, critical infrastructure and supply chains. To date, all applicants for foreign investment permits have received approval from the Committee for Assessing the Reliability of Foreign Investments. Beyond evaluating foreign investments made in Estonia, KAPO also monitors investment applications submitted by other EU member states to ensure they do not compromise Estonia's security interests.

Outbound investments also require careful scrutiny. In 2024, the European Commission initiated the collection of information to support the development of a screening regulation for outbound investments. A potential regulation would seek to prevent the transfer of technology and expertise, with a particular focus on advanced semiconductors, quantum computing, artificial intelligence and biotechnology. It would target technologies crucial to military and surveillance applications.

Innovation

As global technological competition intensifies and Western sanctions on Russia increase, technology-exporting countries aligned with the West have become prime targets for hostile actors. Estonia's academic circles and business sector are also under threat. These hostile states aim to acquire technologies and innovations developed in the West.

If a hostile state gains access to Estonia's advanced technological solutions and expertise, it could potentially enhance its military capabilities. Before forming new partnerships, businesses and academic institutions should ensure that prospective collaborators are not covertly serving the interests of a hostile foreign power. Due diligence should be conducted not only on direct partners but also on their networks and affiliations. Estonian companies must safeguard their proprietary knowledge against information theft and physical and political influence operations.

Methods used to capture innovation:

- **Business and research partnerships, including contract negotiations and technology-focused consultations**
- **Collaborating with universities associated with the defence industry, as well as securing foreign research grants or sponsorships**
- **Enrolling students in higher education institutions located in unfriendly states**
- **Participating in international exhibitions and conferences**
- **Recruiting technical experts to serve as advisers for foreign government and industrial projects**
- **Targeting technical experts for potential recruitment by hostile intelligence services**

If a company suspects that a foreign investor, partner or employee is acting on behalf of a hostile state, it should contact KAPO for assistance.

ANTI-CORRUPTION EFFORTS

Mitigating corruption risks when public officials transition to the private sector is essential to preserving their credibility and maintaining the integrity of the broader administrative system.

Unfair advantages granted by public officials pose a security risk, as they undermine the credibility of governance.

The Supreme Court of Estonia has noted in its rulings that corruption is one of the most challenging crimes to detect, as illicit agreements are typically made in secrecy. In such cases, there are usually no victims in the conventional sense who would report the offence to the authorities, and direct evidence is often lacking. Consequently, criminal proceedings related to corruption frequently depend on circumstantial evidence.

It is deeply concerning when officials entrusted with managing public resources in the best interest of society prioritise private interests over the public good, granting favours to individuals who, in return, further their political careers.

Corruption has no place in Estonian society, and it does not pay off. Court rulings on corruption cases, along with their public coverage, play a crucial role in preventing corruption by demonstrating that the state does not tolerate breaches of integrity and punishes them rigorously.

Conflicts of interest in job transitions

When a public official moves from the public to the private sector, there is no universal code of conduct governing such transitions, which makes it essential to focus on mitigating associated corruption risks.

If an official participates in a public procurement decision-making process and subsequently accepts a job with the winning bidder, this may pose a corruption risk. Suppose a former official moves to a private company to oversee a contract they previously managed, essentially profiting from their own official decisions. In that case, this does not necessarily violate the anti-corruption law; however, it does violate procedural restrictions and contradicts the principles of professional ethics, impartiality and trustworthiness. Subsequent salaries or ownership stakes in a company that benefitted from the official's past decisions may suggest a corrupt arrangement. Officials must avoid situations where their impartiality is called into question, even if only in appearance, as

the public cannot always determine whether the official had prior knowledge of a potential job offer.

For example, best practices on lobbying recommend avoiding situations where an official is rewarded with a position at a lobbying firm in exchange for decisions that benefit that firm, known as the "revolving door effect". The law stipulates a one-year "cooling-off period" after the termination of government employment in cases of direct or constant supervision.[34] However, if no such decisions were made regarding the firm in question, there are no restrictions on future employment.[35]

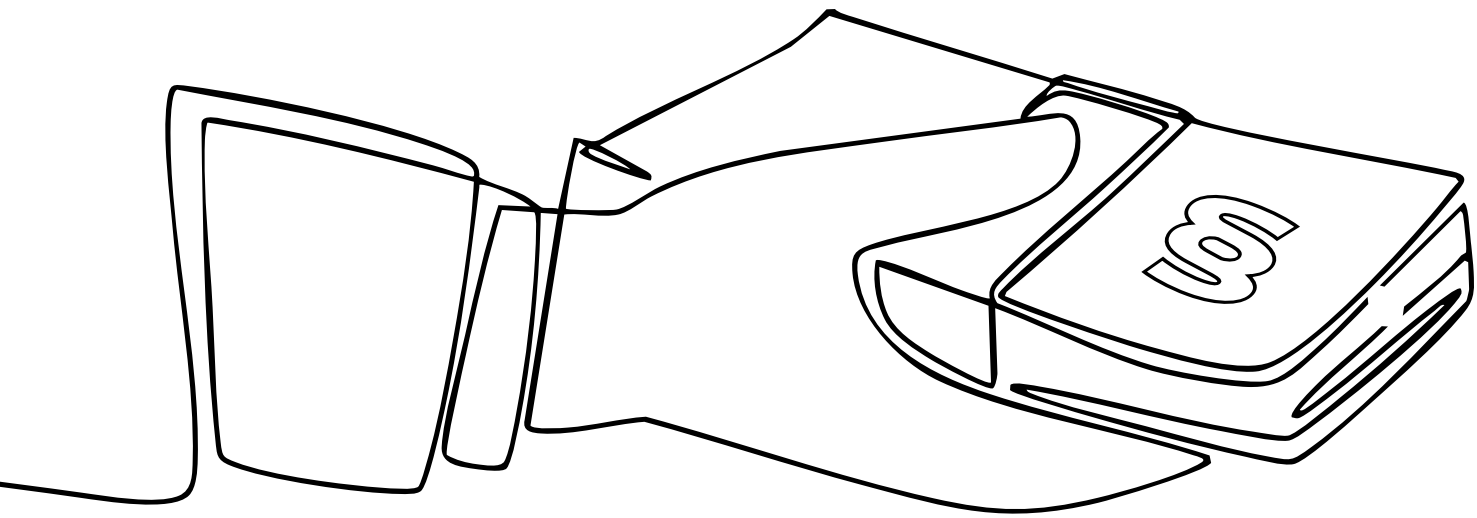
Additionally, the Government of the Republic Act, which entered into force in 2022, stipulates that a government minister must not serve as a member of the management or control body of a legal entity under their ministry's jurisdiction for six months after leaving office. This restriction also applies if the minister made significant decisions affecting that entity's activities or if the entity had contractual relations with the ministry they led.[36]

It would be prudent to establish recommended guidelines for preventing conflicts of interest arising from the revolving door effect. The conditions that should be met when transitioning from the public to the private sector must be defined, and who is responsible for assessing risks, identifying conflicts of interest, and providing guidance on how to avoid them must be determined.

34 The restriction under Section 60(5) of the Civil Service Act establishes a one-year cooling-off period to mitigate the risks associated with the revolving door effect in cases of direct or constant supervision.

35 The issue of revolving doors is regulated by the Civil Service Act, Section 60(5), and the Anti-Corruption Act, Section 7(1–3); it is also partially covered by the recommended best practices for officials engaging with lobbyists.

36 The relevant passage of the Government of the Republic Act is Section 121 regarding the operating restrictions of members of the Government of the Republic after the end of their mandate.



High-risk behaviours can lead to crime

In November 2024, the Harju County Court found Tallinn's former Pirita district governor, Tõnis Liinat, guilty of soliciting and accepting large-scale bribes, embezzlement and violating procedural restrictions.

An investigation by KAPO revealed that Liinat, responsible for overseeing street and green space maintenance in Pirita, demanded bribes from the head of the company contracted for these services. In exchange for the bribes, Liinat ensured the company's success in public procurement procedures and refrained from imposing fines for deficiencies in its work. Previously, Liinat had insisted that his subordinates strictly monitor the company's performance and impose fines for shortcomings. However, after receiving the bribes, the Pirita district government stopped penalising the company.

Liinat effectively cornered the company, presenting it with a difficult choice: either pay ongoing substantial fines or offer him bribes to maintain good relations.

Liinat demanded a total of €53,000 in bribes from the head of the company, of which he received €23,000 before being apprehended by KAPO. Between February and June 2022, the businessman made cash payments to Liinat of €4,000 to €5,000 each month. Liinat quickly spent the illicit funds on high-risk behaviours, which can lead individuals down a criminal path.

The investigation also revealed that Liinat, along with Pirita's head of urban management, arranged for €6,800 worth of landscaping work to be carried out using municipal funds on a private property. To cover up this act, Liinat and the district's head of urban management instructed the contractor to falsely attribute the work to addresses that were public land, despite the soil purchased with taxpayer money never being delivered to those locations.

Liinat was further convicted of violating procedural restrictions. He directed municipal funds towards the construction of a €70,000 noise barrier along Merivälja Road, benefitting individuals who had previously donated €10,000 to his election campaign.

In situations like this, it is crucial to report the issue to law enforcement authorities, who can end an official's corrupt demands. This action not only protects the whistleblower from engaging in illegal activities but also promotes fair competition in the public procurement process.

Liinat admitted partially to the charges brought against him. The Harju County Court sentenced him to four and a half years in prison, of which five months must be served immediately. The court also ordered the confiscation of €20,000 from Liinat.

An unfair or unjustified advantage granted by an official is a security threat

At the beginning of 2025, the Estonian Supreme Court upheld the conviction of former Centre Party Secretary-General Mihhail Korb, businessman Hillar Teder, and the non-profit organisation Eesti Keskerakond (Estonian Centre Party) for influence peddling.

In February 2020, during a meeting at a café in the T1 shopping centre in Tallinn, Teder offered a donation to the Centre Party. In return, he requested that Korb use his influence as the Secretary-General of the Centre Party to pressure his party colleague, Tallinn Mayor Mihhail Kõlvart, into resolving a dispute between Porto Franco, a company linked to Teder, and the City of Tallinn over servitude fees. Specifically, Teder sought to have the fee reduced and the terms, already established by officials, renegotiated.

The circuit court ruled that the evidence clearly showed that Porto Franco was treated differently from standard practice, which was deemed unfair. The interaction between Korb and Kõlvart directly influenced the resolution of the servitude dispute. Porto Franco only began receiving favourable treatment after the meeting between Teder and Korb and their agreement on influence peddling. Had the case followed the standard procedural course and without improper influence, Porto Franco would have had to negotiate with the Municipal Property Department and reach a mutually acceptable agreement. Failing that, the company would have needed to take the matter to an administrative court. The Supreme Court reiterated in its ruling that solely entering into an agreement to influence an official is enough to undermine trust in the integrity of public authorities.

Korb was sentenced to one year and two months in prison, but this sentence was suspended for a two-year probationary period. Teder received a sentence of one year and five months, also suspended with a two-year probation. The court imposed a fine of €750,000 on the Centre Party, which was increased by an additional €250,000 due to an unpaid portion of the fine previously imposed by the Harju County Court. As a result, the total fine for the Centre Party amounted to €1 million.

Source: Estonian Internal Security Service

What is influence peddling?

Influence peddling is a form of bribery, sometimes referred to as criminal lobbying. It involves an intermediary who facilitates the exchange of assets or other benefits between the provider of the advantage and a public official with influence. The crime occurs as soon as an agreement is made to obtain an unfair advantage; the actual transfer of money or benefits is not required for the offence to be complete.

The law prohibits influence peddling to protect the integrity, transparency and impartiality of public administration decisions and actions. Criminalising this practice helps prevent public administration from being dominated by private interests. This law safeguards public trust in executive authority and protects officials from external pressures. It also ensures that all individuals in similar situations are treated equally, preventing anyone from gaining an unfair advantage. Public authority must be not only fair and honest but also perceived as such.

What is a procedural restriction?

In Estonia, public officials are prohibited from making official decisions or performing actions that directly affect themselves or a connected person.

Even if a decision or action does not formally pertain to an official or someone connected to them, any significant financial or personal interest – whether their own or that of a connected person – may still affect their decision or course of action. Therefore, officials are also barred from making decisions or taking action in cases where such interests are present.

Procedural restrictions have been a cornerstone of Estonia's social contract for the past 30 years. Designed to ensure fair and impartial public service, these rules limit the freedom of action of officials who are empowered to make decisions on behalf of the state or local government. In addition to procedural restrictions, officials are barred from using public assets or internal information for personal gain and must not trade official decisions or exert undue influence over other public officials.

The Anti-Corruption Act defines "connected persons" as including an official's family members, close relatives and in-laws. This also extends to legal entities in which the official or their connected person holds at least a 10% stake or has the right to acquire such a stake. Additionally, restrictions apply if the official or their connected person serves on the managing board or supervisory board of the legal entity.

Individuals whose status or activities outside of official duties significantly and directly influence the official are also considered connected persons.

Using public authority for private interests is a security risk

When public officials entrusted with access to sensitive state information and the authority to make critical decisions prioritise private interests over the public good, they become vulnerable to manipulation and undue influence, including from foreign adversaries. As a result, their decisions may be subject to external control or may even be influenced through bribery.

Making decisions based on private interests can significantly increase the costs associated with policy implementation. If officials bypass competitive bidding processes or favour individuals with personal connections, the public will receive fewer services for the same amount of taxpayer money.

If suspicions of corruption arise concerning the proper use of foreign aid, leaders of allied nations and international organisations may conclude that previously granted funds should be repaid and become reluctant to provide further support in the future.

Corruption and dishonest practices undermine public trust in government, weaken social cohesion, and diminish national resilience against external threats, such as military aggression. When corruption is perceived as widespread, people may conclude that fair interactions with the state are impossible and that power is exercised arbitrarily. This perception fosters a culture of bribery throughout all levels of society.

HISTORY

The attempted coup of 1924: A hybrid attack 100 years ago

Although the terms “hybrid warfare” and “hybrid attack” were not commonly used before the 21st century, history provides us many examples of conflicts where military actions were combined with diplomacy, covert operations, political or economic tactics, and information operations to impose one’s will on an adversary.

The Soviet-orchestrated coup attempt in Estonia on 1 December 1924 can be regarded as a hybrid attack. Soviet leaders viewed it as part of the larger goal of a world revolution – the establishment of communist rule across as much of the planet as possible. The Soviet Union relied on Estonian communists, who actively pushed for Estonia to be incorporated into the USSR and throughout 1924 urged Soviet authorities to stage a coup.

On 28 August 1924, the Soviet leadership approved the coup plan, allowing Soviet agencies involved in the operation to begin preparations in cooperation with the Estonian Communist Party. Two command centres were established for this purpose: one operated underground in Tallinn and the other in Leningrad. Both centres included key figures from the Estonian Communist Party, supported by Soviet military intelligence officers of Estonian descent, such as Karl Rimm, Harald Tummeltau and Karl Trakmann. The Leningrad command centre maintained close contact with various Soviet institutions, while Karl Rimm, who was sent to Tallinn, communicated to his superiors through military intelligence channels. The head of Soviet military intelligence, Yan Berzin, personally participated in planning the coup from Moscow.

The operation focused on executing a military offensive. Armed communist strike groups, secretly formed within Estonia, were tasked with carrying out a surprise attack in and around Tallinn, aiming to seize key state institutions. Similar actions were planned in other cities as well. At the same time, combat units were to cross the border from Russia and advance into northeastern and southeastern Estonia to support the takeover. The plan presumed that most Estonian military personnel would remain passive and not resist, while local supporters would reinforce the ranks of the coup forces.

The combat units assembled in the Soviet Union primarily consisted of communists of Estonian and Latvian origin, including some with military backgrounds, and cadets from the Leningrad International Military School. The first wave of the incursion was expected to involve about a thousand lightly armed fighters. If necessary, the operation could have escalated to involve Red Army regular units, as indicated by the late November call-up of four years’ worth of conscripts from the 56th Territorial Rifle Division for training in the Leningrad Military District located across the border from Estonia. However, an immediate invasion by regular forces was not planned; the coup was intended to appear as a local communist uprising, with the Red Army only intervening later in a supporting role.

The Soviet special services – military intelligence and the secret police (OGPU) – provided covert assistance in preparing the military operation. These agencies supplied the strike groups in Estonia with weapons smuggled across the border, which included more than a hundred pistols, hand grenades, various bombs, ammunition and four submachine guns. Most of the weaponry used by the strike groups originated from Russia. Additionally, Soviet special services secretly transported 40 individuals into Estonia to reinforce the strike groups. The majority of these individuals were Estonian communists, some of whom had been transferred from the Red Army and assigned leadership roles within the groups. Those sent to Estonia were given false identity documents issued by the OGPU.

Soviet special services also assisted in planning the operation by supplying intelligence on the positioning and strength of Estonian military units, the activities of Estonian special services, the expected response of the authorities to the coup threat, and other operational details.

The preparations for the coup included information operations. During the summer and autumn of 1924, the Estonian Communist Party secretly printed and distributed leaflets and newspapers throughout Estonia. The materials aimed to prime their supporters for an armed uprising or class war while provoking a militant attitude. A particular emphasis was placed on undermining the morale of the Estonian military. This involved attempts to discredit the senior military leadership and create distrust between conscripts on the one hand and officers and non-commissioned officers on the other. The claims of government abuses, mismanagement of state property, and other wrongdoing within the military were a mixture of truth and disinformation.

Communist propaganda publications also aimed to destabilise Estonia's domestic situation by fabricating claims that right-wing politicians and senior military figures were plotting a fascist coup.

In November, the Soviet press launched an anti-Estonian campaign, using as a pretext the execution of one of the Estonian Communist Party's leading figures, Jaan Tomp, who had been sentenced to death by a Tallinn military tribunal on 14 November. A loud protest was staged outside the Estonian consulate in Leningrad, and in the second half of November, factories and military units in Moscow and Leningrad held rallies adopting resolutions condemning Estonia. These measures were likely intended to psychologically prepare both the Soviet public and military for an imminent invasion of Estonia.

Although Estonian special services had information indicating that the communists were planning a coup, they were unable to pinpoint its exact timing. As a result, when the coup attempt began in the early hours of 1 December, it caught the Estonian side by surprise. The strike groups, numbering around 260–270 people (including nearly 40 who had arrived from across the eastern border and another 40 who worked at the Soviet embassy or other institutions in Tallinn), launched attacks on key locations. Their targets included the Ministry of War, Toompea Castle and the head of state's residence, the Tondi Military Academy, the 10th Infantry Regiment barracks, the Signal Battalion, the tank company barracks and garage, the air division, Balti railway terminal, Tallinn-Väike rail station, the main post office, and several police stations.

In some locations, the attacks were immediately repelled, while in others, the insurgents initially gained a foothold. However, swift and decisive countermeasures by the Estonian military and police ensured that the coup attempt was completely suppressed by midday.

In other cities, the strike groups remained inactive, primarily due to their limited numbers. In Tartu, the relatively large insurgent organisation had already been dismantled in an earlier operation by the Estonian Security Police. Meanwhile, the planned invasion by strike units from the Soviet Union never materialised. At the last moment, Soviet leadership called off the invasion, likely realising that the coup had been poorly prepared and was probably bound to fail. Unwilling to risk the diplomatic fallout of a botched coup, Moscow opted for restraint, wary of straining its relations with major European powers. However, in Tallinn, some strike groups either failed to receive the updated orders in time or chose to proceed regardless – resulting in a complete fiasco.

Reigo Rosenthal

Compiled by:
Marta Tuul

Edited by:
Ave Lepik

Translation:
Refiner

Design:
Ain Kaldra, Andre Poolma (Iconprint)

Photographs:
Estonian Internal Security Service, Facebook, Raul Mee, Scanpix, Shutterstock, Telegram, YouTube

Layout, print:
Iconprint OÜ

(print)
ISSN 2228-1789

(web)
ISSN 2228-1797