

# Risks

Handbook updated 20.11.2025

Downloaded 16.01.2026

# Table of contents

<b>Military threat</b>	<b>3</b>
<b>Hostile special services</b>	<b>5</b>
<b>Infrastructure sabotage</b>	<b>8</b>
<b>Cyber threats</b>	<b>10</b>
<b>Spread of extremism</b>	<b>13</b>
<b>Corruption</b>	<b>16</b>
<b>Money laundering and terrorist financing</b>	<b>17</b>
<b>Illegal mass immigration</b>	<b>20</b>
<b>Mass unrest</b>	<b>22</b>
<b>Sudden attack</b>	<b>24</b>
<b>Floods</b>	<b>26</b>
<b>Forest and wildfires</b>	<b>27</b>
<b>Epidemic</b>	<b>29</b>
<b>Animal disease</b>	<b>31</b>
<b>Large-scale power outage</b>	<b>33</b>
<b>Large-scale communications outage</b>	<b>36</b>
<b>Cross-border nuclear accident</b>	<b>38</b>
<b>Accident handling industrial hazardous chemicals</b>	<b>40</b>
<b>Accident with a radiation source</b>	<b>42</b>
<b>Railway accident</b>	<b>44</b>
<b>Aviation accident</b>	<b>46</b>
<b>Large-scale maritime rescue event</b>	<b>47</b>
<b>Large-scale marine pollution</b>	<b>49</b>
<b>Explosion</b>	<b>52</b>
<b>Building fire</b>	<b>54</b>
<b>Collapse</b>	<b>56</b>
<b>CBRN incident</b>	<b>58</b>
<b>Previously assessed risks</b>	<b>60</b>
<i>Organised crime</i>	<b>60</b>
<i>Transport accident on the road</i>	<b>62</b>
<i>Marine casualty</i>	<b>64</b>

# Military threat



**Threat assessment:** The likelihood of a direct military attack on Estonia in 2025 is considered low, but Russia's policy toward us remains hostile, and its confrontation with Western states continues. Despite enormous losses, Russia's armed forces are growing; it is learning lessons from the war and rapidly developing new capabilities, including drone technology. Compared with the previous risk outlook, the overall threat assessment has not changed.☒

Against the backdrop of the war in Ukraine, Russia is preparing for a long-term confrontation with NATO, with conflict potential that in the medium term also requires strengthening its western border with additional units. Over the past 15 years, Russia's military rhetoric, aggressiveness, and readiness to use military force to achieve its objectives have steadily increased.

Almost certainly, Putin's determination can be explained by the knowledge that losers are not respected in Russia, and therefore – for reasons of prestige alone – he must end the war with an outcome that can be presented as a victory. The Kremlin leader thus remains motivated to find the resources necessary to continue the war, despite costs far greater than originally anticipated and the ever-increasing burden the war places on Russia.

The Kremlin has chosen the path of long-term confrontation and has decided to continue mobilizing additional societal resources both to expand its armed forces and to achieve the goals of military reform. If Russia succeeds in continuing the planned formation of new force groupings under its military reform, Estonia and NATO will in the coming years face a Russian force posture that constitutes a long-term military threat. If the war in Ukraine ends under conditions favourable to Russia, or the conflict is frozen, it is almost certain that more Russian military units will be permanently stationed on Estonia's borders than before 24 February 2022.

## THREATS

- ✓ In the fourth year of Russia's full-scale war of aggression against Ukraine, relations between Estonia and Russia remain predictably at a low point, with no prospect of improvement in the coming years. Russia's objectives and actions toward the Baltic states have not fundamentally changed, but its perception of threat regarding developments in the region has grown.

- ✓ Russia perceives that its strategic position in the Baltic Sea has weakened and its long-term risks have increased, following the start of the war and the accession of Sweden and Finland to NATO. From Russia's perspective, potential risks in the Baltic Sea include the blocking of connections to Kaliningrad and the closure of the Gulf of Finland to maritime traffic. These scenarios demand both preventive measures and the preparation of possible countermeasures.
- ✓ Within a single year, both an army corps and a motor rifle division were formed in Estonia's near vicinity, demonstrating Russia's ability to create large force groupings in a relatively short time. Overall, Russia is expanding its armed forces both nominally – by presidential decree increasing the number of positions in the military – and in practice through recruitment.
- ✓ Russia's defence expenditures in the state budget are breaking records year after year. For 2025, spending on defence and internal security is set to reach nearly 18 trillion rubles, amounting to 40% of the total federal budget. At the same time, there are clear signs that the rapid expansion of defence industry output, fuelled by state funding flows, has reached its ceiling.
- ✓ Based on lessons and experiences from the war in Ukraine, the Russian government has decided to ensure technological and industrial readiness for the large-scale deployment of drone technology. A national drone development program, combined with wartime experience, will likely secure Russian armed forces a strong position in applying drone technology over the long term. After the active fighting in Ukraine ends, Russia will almost certainly apply its experience from drone warfare – as well as its knowledge of the capabilities and weaknesses of Western air defence – when building up forces along the borders with Estonia and NATO.
- ✓ In September 2025, the Russia–Belarus strategic military exercise *Zapad-2025* will take place. The last such large-scale exercise occurred in 2021 (*Zapad-2021*). In the intervening years, Russia has conducted major naval- and air force-centred exercises, for example *Okean-2024* last year.

## ACTIONS

- ✓ NATO has identified Russia as the most serious and immediate threat to the Alliance. NATO must be prepared for immediate collective defence operations across the entire territory of the Alliance. Estonia's military defence is based on both independent defence capability and collective defence. Estonia is a member of NATO and the European Union (EU) and works in close cooperation with allies and other international partners.
- ✓ Estonia continues to accelerate the development of its independent defence capabilities and additional force capacities. In April 2025, the government approved the national defence investment supplementary program KILP, allocating an average of 5.4% of GDP to national defence until 2029.
- ✓ Estonia, together with the EU, NATO, and global partners, provides strong support to Ukraine and

- ✓ continues military assistance until Ukraine has won the full-scale war launched by Russia. By government decision, Estonia will provide Ukraine with annual military aid amounting to 0.25% of GDP from the defence budget during 2024–2027.
- ✓ The accession of Finland and Sweden to NATO strengthens security in the Baltic Sea region. Estonia plays an active role in shaping a new regional security framework that ensures credible deterrence.
- ✓ Within the framework of comprehensive national defence, the entire Estonian society contributes to defence. The aim of Estonia's defence policy is not only to win a possible conflict but to prevent it through deterrence – the most effective and least costly way to defend the country. A whole-of-society approach strengthens Estonia's resilience and readiness for any crisis. As such, comprehensive defence also has a deterrent effect, sending a clear message to any potential aggressor that Estonia is a resilient state and society.

Expand all

[Read more](#)

[International Security and Estonia 2025 – Foreign Intelligence Service](#)

[Be prepared: what to do in a crisis situation – Estonian Rescue Board](#)

Handbook Article last update 11.11.2025

## Hostile special services



**Threat assessment:** The aggressiveness of Russian intelligence services' hybrid activities has increased and may continue to change over the course of the year, but the likelihood of an event directly threatening national security remains low. Compared with the previous assessment, the overall threat level has not changed.

The threat to Estonia's constitutional order continues to stem primarily from Russia's aggressive foreign policy goals. To achieve these objectives more quickly, the Kremlin seeks to destabilize Western societies from within and to weaken the international cooperation that upholds Western values. Russia's strategic aim to expand its influence, is to divide NATO and EU member states by exploiting disinformation campaigns and influence operations to amplify domestic and international problems, undermine trust in Estonia and its allied organizations, polarise communities, and incite tensions between states and peoples.

Toward Estonia, Russia attempts to achieve its goals primarily by manipulating the Russian-speaking community, with particular focus on young people whose mother tongue is Russian. Countering hostile influence activities requires greater domestic and international awareness of influence attempts, methods, and channels, as well as the ability to recognize influence operations and prevent or block the escalation of threats.

In 2024, one of the recurring narratives in Russia's weakened policy of division was to accuse Western states of allegedly widespread and systemic discrimination against Russian-speaking residents. This included politicizing the detention and deportation of Russian citizens who had committed crimes. These are not new tactics in Kremlin propaganda; similar accusations have previously been used to influence domestic politics in the Baltic states and to apply international pressure. However, reputational damage, loss of credibility, and sanctions imposed due to the war have limited Russia's reach in Europe.

## THREATS

- ✓ Since the start of the full-scale war, Russian intelligence services have pursued increasingly aggressive recruitment efforts. The Federal Security Service of the Russian Federation (FSB) has good oversight of individuals entering Russia due to visa applications and border controls. When crossing the border, the FSB frequently inspects people's electronic devices to copy their contents. In addition, people are compelled to provide written statements, signed under obligation, declaring whether they know anyone working in Estonian state services, what their views are on the EU and Ukraine, and whether they know anyone directly involved in combat on Ukraine's side.
- ✓ For decades, Russian intelligence services have cynically exploited the principle of academic freedom in democratic countries, using it for espionage and influence operations. All of Russia's intelligence agencies monitor foreign citizens in Russian universities: practically all international research cooperation projects, as well as foreign students and lecturers coming to Russian universities, are under scrutiny.
- ✓ After Kremlin-controlled information channels were restricted in Estonia, Russia's influence operations shifted to social media. Increasingly, we see deepfakes and manipulations using artificial intelligence and algorithms. Social media is shaping how we perceive the world and directing us into particular information spaces through algorithmic manipulation. As a result, information consumers may find themselves trapped in propaganda echo chambers or minefields of lies, as verifying the authenticity of content becomes ever more difficult.

- ✓ While modern technology offers many methods of gathering intelligence, the oldest method – human intelligence – remains the most widespread. Hostile espionage networks typically target government officials, politicians, businesspeople, journalists, researchers, military personnel, opinion leaders, as well as athletes and youth.
- ✓ Ideological and media cooperation between China and Russia has become closer and more targeted. This cooperation is coordinated at the highest political level, with news reporting considered the top priority. One concrete outcome is the portrayal of the war in Ukraine in a light favorable to Russia within China’s public information space.
- ✓ Investments by Chinese state-owned enterprises (SOEs) in Estonia must be assessed with awareness of their strong political connections and ties to the CCP. The CCP regularly sends inspection teams to overseas branches of Chinese SOEs to oversee party cell activities. This means that the more Chinese SOEs operate in Estonia – alongside private companies with strategic expertise – the greater the risk of technological dependence on China.
- ✓ For the Chinese Communist Party (CCP), international educational and research cooperation plays a special role in strengthening ties between Chinese and foreign universities, with the primary goal of benefiting China’s innovation and technological development. The CCP views education as a key field where China can gain access to Western knowledge through international cooperation.

## ACTIONS

- ✓ To strengthen resilience against hybrid threats, a broad security approach remains necessary. This requires contributions from multiple policy areas and sectors – public, private, and third sector – as well as from communities and individuals, supported by coordinated cooperation. Domestic security needs must continue to be considered in the development of all policy fields.
- ✓ In response to Russia’s aggression in Ukraine and the heightened activity of its intelligence services in Europe, Western states have expelled hundreds of spies working under diplomatic cover from Russian embassies. More recently, intelligence officers posing as scholars, businesspeople, and other professionals have also been arrested.
- ✓ Increasing societal resilience requires not only strategic development of domestic security but also effective education and integration policies and consistent communication by the state. These efforts support stronger cohesion and shared values among different national groups in society, promote mutual understanding, improve knowledge of the national language, expand a shared information space, and strengthen a collective state identity. In this way, risks to security are mitigated alongside other social risks. It is therefore essential to continue a well-considered education, migration, adaptation, and integration policy based on existing principles, and to further develop strategic communication and threat awareness.

Expand all

[Read more](#)

[Annual Review 2024–2025 – Internal Security Service](#)

[International Security and Estonia 2025 – Foreign Intelligence Service](#)

Handbook Article last update 11.11.2025

# Infrastructure sabotage



**Threat assessment:** Deliberate sabotage of critical infrastructure within the next two years is unlikely, but incidents involving damage to undersea connections during this period are considered likely. It is therefore important to accelerate planning for their protection and to implement the necessary regulatory adjustments and additional protective mechanisms.

Since the continuation of Western support and assistance is the key precondition for Russia to subdue Ukraine, the Kremlin has decided to raise the stakes and has launched a deliberate sabotage campaign against Western states, including Estonia. According to Moscow's calculations, the campaign directed by Russian intelligence services is intended to sow fear and confusion and to push Western states decisively away from supporting Ukraine. Another direct goal of the Kremlin is to disrupt and break the supply chains for military and civilian support destined for Ukraine.

Throughout 2024, Europe witnessed arson attacks, acts of vandalism, sabotage, and attempted sabotage carried out under the instruction of Russia's military intelligence service, the GRU. Through hybrid operations, Russia is attempting to destabilize Europe and undermine collective resolve to support Ukraine.

Although it is unlikely that the Kremlin will be able to turn its ongoing sabotage campaign into success in its confrontation with Ukraine and the West, neither the Western political community nor the wider public can ignore Russia's intensified hostile activities. The risks of miscalculation and the inherently violent

nature of the campaign carry too great a possibility of serious consequences, including civilian casualties. For this reason, it is critical for the West to develop adequate countermeasures to deter Moscow's covert freedom of action and prevent further escalation into even riskier hostile behaviour.

## THREATS

- ✓ While most sabotage attempts remain unattributed and some turn out to be accidents, Western states have observed an increase in Russian sabotage attempts. According to the think tank CSIS, the number of Russian attacks nearly tripled between 2023 and 2024. In the case of undersea connections, a cable or pipeline is only one part of the whole system: vulnerable points also include the terrestrial landing sites and control systems. Both China and Russia have the capability to cut undersea cables quickly and cheaply, but so far deliberate sabotage has not been proven in investigations. Russia's shadow fleet consists of old vessels that under normal conditions would have been scrapped. Their crews are poorly trained, inexperienced, and often negligent. In addition to damaging infrastructure, the shadow fleet also poses the risk of potential environmental disasters.
- ✓ Damage to undersea cables in our waters will remain a possibility in the future. All Baltic Sea states are actively cooperating to monitor shipping and vessel activity, to respond quickly and decisively to possible incidents, to collect evidence of criminal intent, and to hold perpetrators accountable.
- ✓ As the aggressor, Russia has demonstrated that energy infrastructure is a target for attacks aimed at lowering societal resilience and morale. Cyberattacks are also a common component of such strategies. By hacking into network management systems used by private companies to control data traffic across cables, cyberattacks can significantly disrupt data flows.
- ✓ Operators of critical infrastructure must maintain and strengthen both physical and digital resilience. A significant number of employees working for providers of essential services still regularly travel to the Russian Federation, despite the Estonian state's recommendation to avoid this entirely.

## ACTIONS

- ✓ On 8 February 2025, a historic step was taken to strengthen energy security – a cornerstone of economic security – when the Baltic states disconnected from the Russian and Belarusian electricity grid and successfully synchronized with the Continental European power system.
- ✓ Crisis preparedness must be maintained and constantly practiced, as the threat of hybrid attacks on infrastructure coordinated by the aggressor state continues to exist. Operators of critical infrastructure must preserve and enhance both physical and digital resilience.
- ✓ Essential service providers must plan for service continuity, assess risks, and prepare recovery

- ✓ plans. They are also required to check the criminal records of employees performing critical tasks. In addition, essential service providers are obliged to notify the competent authority responsible for essential services of any unplanned disruption, interruption, or threat to continuity.
- ✓ In addition to its usual activities, the Estonian Internal Security Service (KAPO) has worked with essential service providers to raise awareness of their vulnerabilities, including those related to supply chains, insufficient adherence to security standards, weak cyber hygiene, or insider threats posed by employees.
- ✓ The European Union and NATO have intensified cooperation on the protection of critical infrastructure, including undersea infrastructure, since the start of Russia's full-scale aggression against Ukraine. A NATO Maritime Centre for the Security of Critical Undersea Infrastructure has been established in the United Kingdom under NATO's Allied Maritime Command (MARCOM). NATO and the EU have also set up a joint working group on critical infrastructure resilience and other cooperation formats. As this area of cooperation is still relatively new, concrete capabilities will need to be developed over the coming years to make it fully operational.

Expand all

[Read more](#)

[Annual Review 2024–2025 – Internal Security Service](#)

[International Security and Estonia 2025 – Foreign Intelligence Service](#)

Handbook Article last update 11.11.2025

## Cyber threats



**Threat assessment:** A successful cyberattack that would significantly affect Estonia's national defence capability, internal security, international relations, vital services, and governance within the next two years is considered likely. Cyberattacks occur constantly, but thanks to protective measures, they have not had a major impact so far. Compared

to the previous assessment, the likelihood of such threats materialising has increased.

The overall global level of cyber and security threats has clearly risen, which has in turn heightened vigilance across society. Attackers' objectives have become more diverse: in addition to cybercriminals seeking financial gain, politically motivated attackers now play an increasingly prominent role in cyberspace.

Technological development offers attackers ever more opportunities, which are exploited not only by profit-driven cybercriminals but also by hacktivists and state-supported cyber groups. All sectors face similar cyber threats, such as denial-of-service attacks, phishing, ransomware, supply chain vulnerabilities, and others. This has been driven by both the increased dependence of services on digital solutions and workforce reductions through automation. The more automated services become, and the smarter the surrounding environment and technology, the more vulnerable these services are to cyberattacks.

In the European Union and other countries, Russian cyber actors have increasingly targeted critical infrastructure, including sectors using industrial automation, as these provide a direct means of influencing the physical world. Cyberattacks against industrial automation systems can have devastating consequences, ranging from equipment damage to extensive disruptions of vital services.

The objectives of cyberattacks may include financial gain, disrupting service availability, cyber-espionage, data theft, and even the destruction of data or infrastructure. Methods include compromising the targeted object (e.g. hijacking user accounts, malicious redirects, spreading/storing malware), affecting availability (e.g. denial-of-service attacks on media outlets), deception (e.g. phishing, financial fraud), and spreading malware (e.g. ransomware, spyware, software manipulation). Some attacks are carried out for political and ideological purposes, such as online propaganda aimed at influencing decision-making. Cyberattacks are generally conducted by criminals and hacktivists, but also by groups with state backing or orders. The impact of cyberattacks varies depending on their complexity and targets.

## THREATS

- ✓ For Estonia and the wider Western world, Russia's war of aggression against Ukraine has significantly increased cyber threats. This has shown that, in addition to supporting kinetic warfare with cyberattacks against critical infrastructure, cyber operations are also widely used as part of hybrid and information warfare. For example, information operations remain a key element of Russia's war of aggression against Ukraine in the cyber domain. Manipulation of information has intensified, likely also because 2024 saw several major events, particularly elections.
- ✓ The threat of supply chain attacks has grown, with attackers compromising software or hardware components embedded in many products. This allows them to gain access to large numbers of

- ✓ organisations worldwide. Attacks through service providers have also become more frequent; for example, compromising a company that provides IT support or accounting services may give criminals access to multiple client networks.
- ✓ Security risks are also increased due to technology from third countries in critical infrastructure. Hardware manufacturers or software developers from states hostile to the West may not always be reliable or well-intentioned. Therefore, when using technology originating from third countries, it is necessary to critically assess the associated risks, plan ways to mitigate them, and/or consider alternative options.
- ✓ In 2024, the number of impactful cyber incidents in Estonia nearly doubled compared with the previous year, rising from 3,314 to 6,515 (a consistent increase in recent years). These mostly involve cases where individuals, institutions, and companies have lost money or data, and information systems have failed due to cyberattacks or technical faults.
- ✓ The incidents that most affect Estonian citizens daily are mass attacks, such as various phishing schemes and fraud (two-thirds of impactful incidents). The sharp increase is largely due to cybercriminals' widespread adoption of artificial intelligence and other automated tools. Using AI for data analysis and natural language processing enables more convincing and personalised fraudulent messages. It also allows attacks to be carried out more quickly and on a larger scale, making them harder to detect and stop. According to Police and Border Guard Board (PPA) data, Estonian individuals and companies lost nearly 8 million euros in 2024 as a result of various fraud schemes – an average of 22,000 euros per day. Risks associated with autonomous superintelligence also need to be considered, including people's limited ability to control and direct its behaviour. The further development of artificial intelligence may create new, previously unknown risks and amplify existing ones, making their mitigation a continuous process.
- ✓ The scale and number of denial-of-service attacks grew significantly in 2024. For instance, in one wave of attacks by Russian hacktivist groups, nearly three billion malicious requests were directed against Estonian public sector websites in just four hours – under normal conditions, such a volume would have taken more than 25 years to accumulate. Denial-of-service attacks targeting Estonia are mostly politically motivated and often focus on services whose disruption would affect the largest number of people. Due to geopolitical tensions, more denial-of-service attacks can be expected in the coming years. Attackers are increasingly targeting internet components critical to overall functioning, such as name servers, cloud services, and authentication services, on which many other web services depend.

## ACTIONS

- ✓ Protecting critical infrastructure and vital services has been the focus of Estonia's cybersecurity efforts in recent years, to ensure that basic needs are met – that electricity, data communication, heating, food, and water remain available, and that hospitals and schools continue to function. The

- ✓ state has helped companies test the security of their systems and has provided training and exercises for their employees. A unique cyber reserve has been created, made up of experts from state IT agencies and the Cyber Unit of the Defence League.
- ✓ Estonia has contributed to creating a safer environment by establishing an Estonian-language security standard (E-ITS), by informing companies about prevalent cyber threats, and by providing training and assistance in incident management. The implementation of information security standards (such as E-ITS or the international ISO27001) helps ensure that a company maintains a suitable level of information security, service continuity, and a good reputation.
- ✓ Cooperation towards a common goal between individuals, institutions, and businesses enables Estonia to respond to cyber threats quickly and flexibly. Our e-services form a network that includes both the public and private sectors, and their security and reliability often depend on one another. Service owners must identify these interdependencies and comply with security requirements throughout the entire lifecycle of their products or services.

Expand all

[Read more](#)

[Cyber Security in Estonia 2025 – Information System Authority](#)

Handbook Article last update 11.11.2025

## Spread of extremism



**Threat assessment:** Although the threat level of terrorism in Europe remains high, in Estonia the risk stemming from the spread of violent extremist ideologies remains low. Compared with the previous assessment, the threat evaluation has not changed.

Any form of violent extremism, regardless of its ideological source, could pose a potential threat to

national security. Although violent right-wing extremists with ambitions of violence have been identified in Estonia – and in January 2025 the first-ever conviction was handed down against three minors belonging to the far-right FKD group – proportionally, the greatest terrorist threat still originates from extremism driven by Islamist ideology. From a broader international perspective, one cannot ignore the regime across Estonia's eastern border, which has been designated as terrorist by both the Riigikogu and the European Union.

People in Estonia who are directly influenced by the Kremlin's hostile propaganda are mostly elderly, and their numbers are declining. The majority of Estonia's Russian-speaking population prefers Estonia's and the West's information and value space to autocratic Russia's. The Kremlin's street-level political support in Estonia is in decline due to sanctions and activists relocating to Russia. For this reason, the Kremlin has been seeking to sustain its divisive policies and shrinking influence by more actively inviting young people from neighbouring countries – whom it deems more easily persuaded – to events in Russia. Since June 2024, the EU's 14th sanctions package against Russia has been in force, which, among other measures, has sanctioned the organisation of the children's camp Artek.

The ideology of Islamist terrorist organisations has not changed over the past decades, nor is it likely to. Their objective remains to replace democratic, universal human rights-based societal structures with ones founded on Islamist religious rules. While Estonia's Muslim community has generally been peaceful, there are signs of radicalisation among its members because of external influences, such as exposure to terrorist propaganda. An important event in this context was the armed conflict between the Palestinian terrorist organisation Hamas and Israel in October 2023, which fuelled a rise in antisemitic sentiment across Europe, including Estonia.

Terrorist propaganda is primarily directed at minors, as they are a vulnerable and high-risk target group. Extremist movements and terrorist organisations exploit young people's digital awareness, their high level of trust in social media, and the user-friendliness of social media applications (including closed communication groups). Young people may lack the background knowledge and critical thinking skills to recognise propaganda, which is increasingly produced with the help of artificial intelligence. As heavy consumers of social media, they are desensitised to violence, and their first encounter with extremist propaganda may not spark immediate interest, but algorithms ensure that the viewed content is shown repeatedly. Influential spokespersons with large followings play an important role. Such spokespersons use public channels to define the "correct and permitted" connections between Islam and secular life, as well as the behaviour of the "true believer" or "true warrior." This kind of messaging pushes audiences towards supporting extremist views of society.

## THREATS

- ✓ Illegal transit of combat weapons into Europe poses a threat, where they may fall into the hands of criminal networks and extremists.
- ✓ The development of artificial intelligence is changing the threat landscape. New tools make it possible to deliver fluent hate messages in Estonian and constantly improving AI applications make

- ✓ hate content appear increasingly convincing. For this reason, source-checking measures in media organisations, as well as media literacy in society, are becoming ever more critical in preventing hostile information from taking hold in Estonia.
- ✓ Another threat is the dissemination of terrorist propaganda on public social media. While this is prohibited under the EU regulation aimed at curbing the spread of terrorist online content, the circulation of such content within closed social media applications and chat groups remains outside the regulation's scope.
- ✓ Foreign fighters travelling to conflict zones have used Estonia as a transit country, either on their way to the conflict area or returning to Europe. Belarus's hybrid attack through migration and the mass immigration resulting from the war in Ukraine have increased the need to prevent dangerous individuals from entering at the state border and to strengthen border protection.

## ACTIONS

- ✓ Because of the propaganda activities of hostile states and the spread of violent extremism, Estonia must pay closer attention to what occurs on social media platforms (including in closed groups). Although the threat of terrorism remains low in Estonia, even a single attack would be one too many.
- ✓ A key factor in preventing violent extremism and mitigating threats is social cohesion and a sense of belonging within society. As a result of Russia's war of aggression, economic downturn, and the rising cost of energy and food, the risk of radicalisation among Islamist, right-wing, and left-wing extremists in Estonia may increase. Extremist views do not emerge overnight; timely detection of radicalisation, as well as the prevention and interruption of related risk behaviour, is only possible through nationwide cooperation.
- ✓ It is vital to train frontline officials and professionals who work directly with citizens (in law enforcement, corrections, integration, education, and social sectors), as well as the wider public, to recognise signs of radicalisation. Therefore, it is essential to continuously develop the relevant capacities of law enforcement and supervisory authorities, and in cooperation with the relevant ministries, agencies, and the private sector, to promote online safety.
- ✓ Within the framework of its radicalisation prevention action plan, Estonia is creating an intervention model to support individuals in moving away from extremism and towards deradicalisation. One of the objectives of this action plan, spearheaded by the Ministry of the Interior, is to prepare training materials and guidelines to help, for example, people working with young people to detect extremism, but also to prevent it through their everyday work.

[Read more](#)

[Annual Review 2024–2025 – Internal Security Service](#)

Handbook Article last update 11.11.2025

# Corruption



**Threat assessment:** The occurrence of large-scale corruption in Estonia is considered unlikely. Compared with the previous assessment, the threat evaluation has not changed.

The Supreme Court of Estonia has noted in its rulings that corruption is one of the most difficult crimes to detect, as unlawful agreements are usually made in secret. Such crimes generally lack victims in the conventional sense, which means there are usually no individuals willing to report them to the authorities. Direct evidence may be absent, and therefore, investigations into corruption offences often must rely primarily on indirect evidence.

Corruption creates inequality and reproduces poverty through the government's distorted spending. It also goes hand in hand with political and economic instability. As a result of corruption, economic growth declines because a corrupt economic environment does not encourage investment. Corrupt organisations fail to function and to fulfil the purposes for which they were established – for example, a corrupt judge does not administer justice, a corrupt police officer neither prevents nor halts offences, and a corrupt politician does not act in the interests of the state, but instead pursues personal business or other private interests. A corrupt business environment also affects the consumer, who faces fewer or more expensive choices.

Professional decisions influenced by private interests can significantly increase implementation costs. By bypassing or rejecting competitive tenders and favouring a person with whom one is connected, the result is that the same money buys fewer public services. If corruption casts doubt on whether foreign aid allocated to the state is being used appropriately, this may affect the leaders of allied countries and

international organisations. It could lead to decisions to reclaim funds already provided and to refrain from offering support in the future.

The spread of corruption as dishonesty undermines the credibility of the state among its citizens, weakens social cohesion, and thereby reduces the country's resilience against external threats, including military aggression. If corruption becomes widely perceived as the norm and people come to believe that it is impossible to deal with the state honestly and that power is wielded arbitrarily, bribery and influence-peddling will flourish at every level.

## THREATS

- ✓ Estonia's economic environment is still under recessionary pressure, meaning that in 2025 an increase in property crimes as well as tax and bankruptcy offences committed by companies can be expected. The economic situation also increases the risk of corruption offences, as entrepreneurs may have a greater incentive to secure a guaranteed turnover.
- ✓ In Transparency International's 2024 Corruption Perceptions Index, Estonia, with 76 points, shares 13th place with Uruguay. Over the past ten years, Estonia's score has improved by six points, but in recent years progress has stalled. The Corruption Perceptions Index shows that most countries have made no progress in combating corruption over more than a decade, or have not achieved any success at all, and more than two-thirds of countries scored below 50 out of 100.
- ✓ Transparency International has highlighted the link between corruption and the climate crisis. Due to a combination of factors, the often highly ambitious measures needed to slow climate change are not adopted at the political level, with the narrow business interests of specific groups being prioritised over the common good. Therefore, maintaining a low level of corruption in society clearly contributes to long-term plans aimed at ensuring environmental sustainability.

## ACTIONS

- ✓ GRECO – the Group of States Against Corruption – is an anti-corruption association of states operating under the Council of Europe. GRECO's objective is to assess the readiness of member states to combat corruption and, through its evaluation procedure, to provide countries with recommendations for anti-corruption measures. Estonia has successfully completed the five evaluation rounds carried out so far. The sixth evaluation round, beginning in 2025, will assess anti-corruption activities in local governments.

# Money laundering and terrorist financing



**Threat assessment:** The occurrence of a large-scale event involving money laundering and terrorist financing is considered likely. The assessment has not changed compared with the previous year.

Estonia's money laundering risk landscape is shaped by the trend of crime becoming more international and networked, with criminals making use of professional money laundering networks and seeking individuals and companies around the world willing to participate temporarily in specific criminal projects. In the Estonian context, there are indications of international criminal networks being active, particularly in relation to fraud, tax offences, and the subsequent laundering of illicit proceeds. The money laundering threat in Estonia is also linked to the increasingly tense geopolitical situation. Russia continues its aggression in Ukraine and hybrid attacks in Europe. Such activities require funding, which is why the movement of money or its equivalents through Estonia's financial system must be monitored especially closely.

Sanctions imposed on Russia are forcing criminals to adopt more complex methods to evade restrictions on trade and financial flows. Both traditional money laundering methods and international laundering networks are used to circumvent sanctions. Russian intelligence services and organised crime groups are known to cooperate in order to evade sanctions, exploiting existing laundering infrastructures as well as cryptocurrencies. In 2024, the Estonian Financial Intelligence Unit (RAB) observed laundering of money earned through sanction violations in the cases it analysed.

The number of suspicious transaction reports (STRs) submitted to RAB, as well as the amounts involved, were on the rise in 2024. At the same time, the identified volume of laundered money was still in decline: in 2024, RAB forwarded suspicious transactions worth a total of €222 million to investigative authorities, representing a 19% drop compared with 2023, and the number of such transmissions fell by 29%. The main predicate offences indicated in these reports were sanction evasion, tax offences, and fraud. Compared with previous years, cases linked to corruption and embezzlement stood out more clearly. As before, the majority of RAB's reports concerned so-called autonomous money laundering, where there were no direct indications of predicate offences, but the activity patterns strongly suggested laundering. International information exchange continued to focus primarily on fraud-related money laundering, although this showed a declining trend.

Thanks to the work of Estonian supervisory authorities, the number of high-risk market participants has decreased among credit institutions, virtual asset service providers, financing institutions, and corporate service providers. The money laundering risks of these sectors have become concentrated in the hands of a few participants with higher-than-average risk appetite and more international clientele, several of

whom have seen significant growth in cross-border transaction volumes. The inherent risk of the gambling sector is increasingly coming to the fore, particularly in relation to internationally licensed online casinos and sports betting platforms operating in Estonia. Both financial and non-financial obligated entities remain vulnerable due to the presence of unlicensed operators in their sectors.

Estonia's terrorist financing risk landscape is primarily shaped by correspondent relationships. It is mainly through such arrangements that the majority of suspected terrorist financing cases originate. This is evident both in the banking sector and among virtual asset service providers. In both cases, Estonia's jurisdiction and open economic environment are exploited. Transactions are carried out through the Estonian legal-entity customer of the service provider (the respondent institution), which itself operates in another jurisdiction. The client of that respondent institution – usually a natural person residing abroad – is typically the one sending the funds.

The quality of reports submitted to RAB concerning suspected terrorist financing improved significantly in the years leading up to 2024, but since then progress has slowed. In 2024, the total number of such reports was about one-third lower than in the couple of years before. Some sectors still do not submit any relevant reports at all, such as non-profit organisations, while others submit them with insufficient quality, such as some virtual asset service providers.

## THREATS

- ✓ The greatest threat for Estonia remains the layering of criminal proceeds obtained abroad within Estonia's financial system, particularly when used to circumvent and violate sanctions against Russia. Cross-border layering of illicit funds continues to pose the highest risk to payment services provided by credit institutions, especially regarding correspondent services to foreign fintech providers. Since 2021, the total sums of cross-border transactions reflected in RAB reports have grown markedly. According to reports, the main destination countries for suspicious funds were Lithuania, the United Kingdom, Poland, Bulgaria, and Switzerland, while the main source countries were Lithuania, Germany, Latvia, Finland, the United Kingdom, and Poland.
- ✓ Estonian legal entities, especially private limited companies (OÜs), are exploited in international criminal schemes (mainly tax offences, fraud, and associated money laundering). In many cases, these suspicious transactions do not involve Estonia's financial system at all. RAB frequently receives information about suspicious transactions by Estonian persons conducted through payment accounts in foreign banks and e-money institutions. Lithuanian payment accounts still predominate in RAB's reports, but in terms of transaction volumes, accounts held by Estonian persons in Belgium, Malta, the United Kingdom, Austria, and Germany also stand out.
- ✓ In the context of terrorist financing, Estonia's main risk concerns money transfers to Tajikistan, Kyrgyzstan, and Turkmenistan. Estonia's competent authorities added these three states to the list of countries with elevated terrorist financing risks.

- ✓ Donations linked to the Hamas–Israel war continue to affect Estonia’s risk landscape. The threat has materialised in correspondent relationships of credit institutions, where donations from abroad can be directed to foreign non-profit organisations through payment service providers.

## ACTIONS

- ✓ The Financial Intelligence Unit (RAB) continuously analyses the risk environment and prepares and publishes strategic analyses. Supervisory authorities assess the risks linked to their regulated entities and to specific sectors. Market participants themselves are also required to assess the risks inherent to their field of activity and to implement mitigation measures.
- ✓ Competent authorities organise the registration and licensing of market participants and oversee their compliance. Market participants are required to build organisational systems to prevent money laundering and terrorist financing, including applying due diligence measures and fulfilling reporting obligations.
- ✓ In response to emerging trends in financial crime and the increasing complexity of money laundering as a concealed offence, more technologically advanced solutions must be used for detection. In the field of anti-money laundering and counter-terrorist financing, data-driven risk assessment and decision-making are essential. The demand for better data analytics necessitates the development of data management and the creation of the necessary legal environment, on which RAB has been actively working.

Handbook Article last update 11.11.2025

# Illegal mass immigration



**Threat assessment:** The risk of mass immigration to Estonia is low, and it is unlikely to develop into a crisis within the next two years. Compared with the previous assessment, the risk level has decreased – from very likely to unlikely.

At present, the threat of mass immigration to Estonia is considered low. However, it must be acknowledged that Russia has the capacity to create migratory pressure at Estonia's eastern border. In preparing its capabilities, the Police and Border Guard Board (PPA) takes into account the obligation set out in the migration package, which requires the ability to process 187 individuals per day and 748 per year. From the state's perspective, drawing on the experience of the Ukraine crisis, it is possible to manage a situation in which up to 50,000 migrants arrive in Estonia over two to three months, provided that the country of origin of the refugees is cooperative. At the same time, crises are also defined as deliberate and systematic migration attacks directed at Estonia's border, with the aim of exhausting the resources of the security authorities. Such events create the need to localise, register, identify, accommodate or detain, and if necessary, deport a large number of people.

Although pressure from illegal migration on the EU's external borders decreased by almost 40% in 2024 compared with the previous year, it cannot be claimed that the EU has become a less attractive destination for migrants. The reduction was supported by additional border controls and cooperation with third countries. Nevertheless, pressure on the EU's external borders persists, although it is unlikely to increase significantly.

It is beyond doubt that Russia's desire to continue and expand its influence operations and hybrid activities at the EU's eastern border will remain in the future.

## THREATS

- ✓ Although the situation at Estonia's border is relatively calm as of spring 2025, it could change at any moment. Russia has both the capacity and the interest to continue hybrid operations (including migration attacks) and divisive activities aimed at Western states.
- ✓ Russia's actions have so far shown that it is creative in planning and carrying out such operations, and constant testing of Estonia's border guard capabilities and responses continues at the eastern border.
- ✓ Russia and Belarus remain attractive to migrants thanks to simplified visa regimes and direct flight connections. Migration pressure persists especially at Estonia's eastern border, which now also sees migrants arriving from Africa, the Middle East, and South Asia.
- ✓ Even though Russia has avoided creating a larger flow of migration towards Estonia's border, Estonia's eastern frontier and the events taking place there remain part of Russia's broader strategy aimed at undermining unity in Estonian society and in Western countries more widely.

## ACTIONS

- ✓ Estonia is creating a crisis reserve of 1,000 reservists, composed of former military police conscripts, whose task will be to assist the police in the event of a migration attack or domestic unrest.
- ✓ Situational awareness is ensured through the assessment of internal and external threats in order to forecast the likelihood of such events.
- ✓ Risk communication is conducted, and the public is informed about the causes of migration and the dangers associated with it.
- ✓ Schengen compensatory measures are implemented to check the legality of individuals' stay throughout the territory of Estonia.
- ✓ Border control is strengthened by the development of the eastern border infrastructure.
- ✓ The guarding of the border and of critical sites is further developed.

Handbook Article last update 11.11.2025

# Mass unrest



**Threat assessment:** The occurrence of mass disorder in Estonia is unlikely. Compared with the previous assessment, the threat evaluation has not changed.

In recent years, the main causes of mass protests in Europe have been political developments and/or decisions concerning the economy, security, or climate. In 2023 and 2024, farmer protests driven by the green transition spread across Europe, although there were also other causes, such as extreme weather conditions, cheap imports, and the lack of support systems. Demonstrations may also be sparked by isolated incidents that take place elsewhere (for example, the Black Lives Matter movement, which

spread from the United States across Europe).

In Estonia, no demonstrations or public gatherings have escalated into mass disorder for over a decade. The largest gatherings in recent years have been primarily related to decisions and activities during crises and in the field of security.

A trend of increasing registered demonstrations can be observed. The main influencing factors are changes in the security environment and people's living standards, which means that demonstrations with the potential to escalate into mass disorder are above all reactions to political decisions. A triggering factor may be the media coverage of a given event as well as deliberate influence operations by hostile states.

## THREATS

- ✓ People's living conditions have worsened, dissatisfaction has grown, and this continues to be exploited in political power struggles, leading to a significant increase in the number of mass gatherings.
- ✓ The April 2007 riots showed that developments and political decisions in society are exploited in the influence operations of the Russian Federation. Social disagreements and opposition are seized upon and channelled, which can lead demonstrations to escalate into clashes and disorder.
- ✓ Mass disorder resulting in casualties most often occurs in confrontations between demonstrators and the police. In such events, the decisive factor is the presence of individuals with malicious intent who deliberately seek to turn a peaceful protest into a violent situation.
- ✓ People now receive information from entirely different and fragmented sources, subject to far less oversight than before. Since there are so many channels, the level of information noise is high, making it more difficult for individuals to distinguish false information from accurate facts.

## ACTIONS

- ✓ Capabilities for detention and mass control are being developed, including through the crisis role of assistant police officers. Estonia is also creating a crisis reserve of 1,000 reservists, composed of former military police conscripts, whose task will be to support the police in the event of a migration attack or domestic unrest.
- ✓ Situational awareness is ensured by assessing internal and external threats in order to forecast the likelihood of such events.

- ✓ Risk communication is carried out, and the public is informed about the causes of disorder and the dangers associated with it.
- ✓ Processes related to the handling of offences are being further developed.

Handbook Article last update 11.11.2025

## Sudden attack



**Threat assessment:** The likelihood of a sudden attack occurring in Estonia is low. Compared with the previous assessment, the risk evaluation has not changed.

A sudden attack is an event in which one or more individuals, using a suitable means, attempt within a short period of time in a crowded place to injure or kill as many people as possible or cause as much damage as possible. Terrorist attacks account for only about one-third of all sudden attacks.

Violent ideologies rooted in any form of extremism often attract young people with mental health or family-related problems. As mental health deteriorates, the probability of carrying out a sudden attack increases. Some young people who are interested in terrorist ideologies are active online, showing greater ideological flexibility and readiness to use violence. Certain vulnerable young people are also direct targets of active recruitment. Lone actors are usually not completely isolated; more often, they are young individuals integrated into online communities that promote violence.

### THREATS

- ✓ Events in recent years worldwide – war, inflation, rising prices, worsening living standards, and growing societal tensions – have created fertile ground for the spread of violent extremism. Radicalisation can occur covertly and quickly, making it difficult to assess the probability of an

- ✓ attack.
- ✓ The most likely triggers for attacks are family and psychological problems or mental illnesses. Factors that can lead an individual to attack include depression, suicidal thoughts, feelings of persecution, desires for revenge, romantic grievances, or the wish to gain attention.
- ✓ Other reasons for sudden attacks are generally social, economic, or personal in nature, with attack targets typically linked directly to these causes.
- ✓ Terrorist and violent extremists are capable of strategically integrating digital technology – including the latest developments in artificial intelligence – into their toolkit to spread propaganda, recruit members, plan attacks, and avoid detection by law enforcement agencies.

## Guidelines

If you witness a sudden attack in a public place, or notice a situation that may indicate the possibility of such an attack:

- ✓ Leave the dangerous area quickly and seek cover.
- ✓ Once you have reached a safe location, call the emergency number 112.
- ✓ If possible, warn others.
- ✓ Follow the instructions and orders of the police.

### **Remember:**

- ✓ The attacker may injure anyone in their path.
- ✓ The attacker cannot be persuaded to stop.
- ✓ The first 10 minutes are critical for your survival.
- ✓ Attackers may, but do not necessarily, take hostages.

Expand all

[Read more](#)

EUROPOL – [European Union Terrorism Situation and Trend report 2024 \(EU TE-SAT\)](#)

Handbook Article last update 20.11.2025

# Floods



**Threat assessment:** The occurrence of a severe flood in Estonia is considered likely. Due to climate change, the risk of flooding is increasing, and as floods occur with a certain frequency, the probability of a flood with serious consequences has risen compared with earlier years. Compared with the previous assessment, the threat level has increased from unlikely to likely.

Flooding in Estonia can arise primarily from rising water levels in inland bodies of water and the sea, but also in areas not directly connected to water bodies, where the soil is unable to absorb water from heavy rainfall or snowmelt. It can also occur in urban settlements where surfaces are covered with impermeable materials. In recent years, stormwater flooding has been frequent in urban areas. Most towns and cities are covered with impermeable surfaces, such as asphalt or buildings. The denser and more impermeable the urban space, the greater the probability that such floods will occur.

The rise in water levels in inland water bodies is mainly caused by the spring floods, including ice jams formed by the accumulation of drift ice. In Estonia, 34 densely populated risk areas have been identified that are expected to be affected in the future by rising sea levels and inland water flooding.

On Estonia's coastal areas, as elsewhere in the eastern Baltic Sea, water level rise is caused by strong south-westerly and westerly storms. These storm surges are sharp, short-lived (lasting 1–2 days), and localised.

## THREATS

- ✓ Climate change forecasts indicate that in the 21st century, storms in the Baltic Sea region will become more frequent, and consequently the risk of flooding caused by rising sea levels will increase. The melting of continental ice sheets and the thermal expansion of the oceans have already accelerated the rise of global sea levels, and this rise is projected to intensify further throughout the 21st century.
- ✓ Forecasts also indicate both an overall increase in average annual precipitation and an increase in the frequency of extreme rainfall events, especially in the summer months. Heavy, intense downpours are expected to cause local flooding particularly in urban areas with large impermeable surfaces.
- ✓ By the end of the 21st century, a significant reduction in snow cover is projected, together with an overall increase in average precipitation. This suggests that spring river floods caused by snowmelt may increasingly be replaced by floods in autumn resulting from heavy rainfall.

## ACTIONS

- ✓ To mitigate flood risks, Estonia prepares a flood risk management plan, designates risk areas, and maps potential flood hazards.
- ✓ Preventive measures against flooding mainly involve spatial planning regulations and the preparation of information to support planning decisions.
- ✓ Protective measures against floods require the designation and implementation of various technical solutions. These include the construction of embankments or other traditional protective barriers, as well as the protection of technical equipment, improvements in drainage, or the redirection of water flow.
- ✓ It is also necessary to ensure preparedness for floods. This means taking measures to safeguard the population and prevent environmental damage during a flood, ensuring the functioning of flood forecasting and warning systems, and raising public awareness.

# Forest and wildfires



**Threat assessment:** The occurrence of a large-scale forest or landscape fire in Estonia is unlikely. However, as climate warming continues, the risk of forest and grassland fires is increasing. Compared with the previous assessment, the threat evaluation has not changed.

The fire hazard in forests depends on the forest site type, age, and the tree species growing there, on the basis of which forests are classified into fire hazard classes. The highest fire hazard class applies to coniferous forest stands, while deciduous forests are categorised as having the lowest fire hazard.

According to data from the past three years, in about 95% of forest and landscape fires the burned area has remained below three hectares. Larger fires have been prevented by active prevention work and by the rapid and appropriate response of rescue teams. Fires in which the burned area was at least 10 hectares numbered 19 in total, representing only 1% of all forest and landscape fires. Since 2018, no large-scale forest or landscape fires have occurred in Estonia.

Weather conditions are a key factor in forest and grassland fires. Low rainfall, strong winds, high air temperatures, and low humidity increase fire risk and promote the rapid and extensive spread of fires.

## THREATS

- ✓ In nearly half of cases, the cause of forest and wildfires remains undetermined. Of the identified causes, only 1–3% were the result of natural phenomena, meaning that most of the identified causes were human-related. The most common among these are non-compliance with fire safety requirements when making bonfires and the burning of dry grass. Other identified causes include electrical equipment and installation faults, smoking, children playing with open flames, and barbecuing, although these occur less frequently.
- ✓ Fires started by motor vehicles are mostly linked to agricultural work, for example sparks from tractors or combine harvesters, peat processing, and driving motor vehicles on peat surfaces.
- ✓ Most forest and grassland fires occur primarily in Harju County (34%), Ida-Viru County (18%), Pärnu County (8%), and Tartu County (8%), where population density is also higher than average.

- ✓ Heatwaves and droughts are becoming more frequent and lasting longer. As a result, in the future the number of forest and grassland fires and the extent of burned areas may increase. The projected rise in the number of fire hazard days is expected to stem mainly from increased evaporation in a warmer climate, which reduces soil moisture content. In addition, earlier snowmelt in the future could cause the fire season to begin earlier.

## GUIDELINES

If you discover a forest or wildfire:

- ✓ Immediately notify the emergency center by calling 112, where the fire has broken out and what is burning.
- ✓ Warn people in danger.
- ✓ If you are sure of your safety, start extinguishing the fire or preventing the spread of the fire as much as possible.

Handbook Article last update 20.11.2025

# Epidemic



**Threat assessment:** The introduction of an infectious disease with high potential for spread (especially droplet- or airborne viral infections) from abroad and its extensive dissemination in Estonia is very likely. Epidemic spread of vaccine-preventable diseases is unlikely, given the level of vaccination coverage in the population. Compared with the previous assessment, the probability of a new pandemic emerging and spreading has increased from likely to very likely, considering the high mutation capacity of pandemic-potential viruses, their rapid spread, increasingly effective adaptation mechanisms for

transmission to humans, and the frequent absence or weakness of population-level immunity. At the same time, the probability of epidemic spread of vaccine-preventable diseases has decreased from unlikely to very unlikely.

Epidemics may be caused by pathogens of various origins, particularly viruses or bacteria transmitted through contaminated air, food, water, droplets, airborne particles, or direct contact. Diseases with very high or high epidemic potential include droplet- and airborne-transmitted infections such as measles, COVID-19 and other coronavirus infections such as MERS and SARS, influenza, as well as contact-spread haemorrhagic viral fevers such as Ebola and Marburg, and also hepatitis A, Escherichia coli infections, and others. An epidemic can develop very rapidly in today's conditions of intensive international travel, particularly when a new virus emerges. The spread of a virus can become extensive quickly, since in the initial phase its nature is often unknown – specific diagnostic tools, effective treatments, and suitable containment measures may be lacking. As a result, it is difficult to detect and control cases in time, creating favourable conditions for rapid viral transmission before intervention measures can be applied.

The probability of a new pathogen emerging in Estonia is very low. However, the likelihood of a new pathogen – especially a virus – arising is greater in regions with higher population density and more frequent contact between humans and different animal and bird species. The population is vulnerable to the spread of a new pathogen, as there is no prior exposure or immunity.

## THREATS

- ✓ Year by year, anti-vaccination attitudes have deepened, with an increasing number of parents refusing to vaccinate their children, thereby raising the risk of outbreaks of vaccine-preventable diseases.
- ✓ Vulnerable population groups for several infectious diseases include people with chronic illnesses and weaker immune responses, the elderly, pregnant women, and young children.
- ✓ A growing global problem is the ability of pathogens (viruses, bacteria, fungi, protozoa) to become resistant to available treatments. This creates a situation where an infectious disease no longer responds to standard medical therapies, and diseases may emerge whose spread we can no longer control.
- ✓ Unfortunately, science cannot precisely predict the timing of viral mutation processes. Annual seasonal spikes in illness confirm that viruses mutate continuously. When viruses undergo complete genetic structural changes, disease may spread epidemically, cause a rapid and simultaneous increase in the need for hospitalisation, and disrupt the provision of vital services.

- ✓ Increased international travel may raise the likelihood of importing cases of disease. The manifestations and probability of such risks may also be affected by complex security and economic-political conditions, which could be accompanied by large-scale migration.
- ✓ Climate change significantly influences the spread of infectious diseases, as it alters environmental conditions in ways that facilitate the spread of pathogens and their vectors into new areas. Rising temperatures, changes in rainfall patterns, and higher humidity create better conditions for ticks and mosquitoes, enabling them to remain active for longer and extend their habitats further north.

## ACTIONS

- ✓ Preventing epidemics requires a strong and well-functioning monitoring system. The Health Board monitors and analyses the spread of pathogens, including viruses, and the epidemiological situation both in Estonia and internationally. Preparedness plans have been developed to minimise disease spread.
- ✓ The Health Board's website provides systematic and regularly updated information on infectious diseases, including brief descriptions, prevention, and containment measures.
- ✓ In Estonia, 14 infectious diseases are covered by the national immunisation programme.
- ✓ Regular campaigns are carried out to influence vaccination behaviour and provide vaccination recommendations, and a dedicated website ([vaksineeri.ee](http://vaksineeri.ee)) has been established.
- ✓ Estonia has developed vaccination plans to ensure rapid and accessible immunisation for all in the event of possible epidemics or pandemics. The state participates in joint procurement initiatives of the European Union, ensuring fast access to vaccines when necessary. National medicine reserves have also been created to guarantee the availability of essential medicines in crisis situations.

## GUIDELINES

Preventing the emergence of an epidemic and coping during one requires the contribution of everyone. It is important to follow national behavioural guidelines and to avoid all contact with others if there is any suspicion of infection.

# Animal disease



**Threat assessment:** The occurrence of a large-scale animal disease outbreak in Estonia is considered likely. Compared with the previous assessment, the probability of such an event has increased from unlikely to likely.

The years 2023 and 2024 were stable in terms of the occurrence of animal diseases. No particularly dangerous animal diseases were detected in kept animals, and there were no changes in the statuses of animal diseases subject to official eradication programmes.

The particularly dangerous animal diseases affecting terrestrial animals include Newcastle disease, cattle plague (rinderpest), foot-and-mouth disease, African horse sickness, highly pathogenic avian influenza, sheep and goat pox, lumpy skin disease, Rift Valley fever, African swine fever, classical swine fever, contagious bovine pleuropneumonia, contagious caprine pleuropneumonia, ovine rinderpest, and glanders. For aquatic animals, five diseases are classified as particularly dangerous, of which in Estonian conditions the most significant is epizootic haematopoietic necrosis, which threatens rainbow trout and perch.

## THREATS

- ✓ Particularly dangerous animal diseases may also be transmissible to humans, causing illness or even death. Veterinarians and people working in outbreak sites are especially at risk if they do not use personal protective equipment in a timely or sufficient manner.
- ✓ Although inspections in animal husbandry facilities show a decrease in the number of detected violations, at the same time the practice of free-range keeping of animals and birds is increasing, as is people's unrestricted movement between animal and poultry farms. This creates favourable conditions for the spread of infections from one farm to another. In addition, animal diseases are spreading in Europe that had either not occurred before or had not been seen for decades.
- ✓ African swine fever (ASF) remains endemic in Estonia. In recent years, the wild boar population has been increasing. While in 2018 the winter population was just over 5,000 wild boar, by 2024 it had risen to nearly 17,000 individuals. The most recent outbreaks in domestic pigs occurred in July 2023 in two farms in southern Estonia. ASF has also been diagnosed in Estonia's neighbouring and nearby countries: Latvia, Lithuania, Poland, and the Russian Federation. In 2024, 21 European countries reported ASF outbreaks.

- ✓ Compared with several previous years, the number of highly pathogenic avian influenza outbreaks has risen in Europe, including in the Nordic countries, meaning that the risk of the disease spreading from wild birds to domestic poultry is significantly higher. Detection of avian influenza viruses in mammals is also on the rise.

#### ACTIONS

- ✓ As part of national animal disease programmes, herds in Estonia are examined annually for more than 36 animal diseases to determine their presence or absence. In addition, planned official inspections of livestock holdings are carried out on a risk basis to monitor their general compliance with established requirements.
- ✓ In April 2025, the Estonian Agriculture and Food Board commissioned two expert opinions from the National Centre for Laboratory Research and Risk Assessment. These opinions concluded that the risk of introducing foot-and-mouth disease into Estonia is not high.
- ✓ The Agriculture and Food Board considers it extremely important and necessary to raise awareness among both animal keepers and the wider public.

#### GUIDELINES

Everyone can contribute to preventing the spread of animal diseases:

- ✓ Do not bring animal products from abroad that may be contaminated with pathogens.
- ✓ Avoid, where possible, contact with farm animals and wild animals. If you visit a farm, wait at least 48 hours before going to another farm.
- ✓ Vaccinate your pets against rabies and do not bring unvaccinated pets into the country.

Handbook Article last update 20.11.2025

# Large-scale power outage



**Threat assessment:** A widespread power outage in Estonia is very likely. Compared to the previous assessment, the risk rating has not changed.

In the main grid, the impact of power outages has decreased over the last decade. The main causes have been technical failures or severe weather conditions.

In the distribution grid, the number of outages decreased over the past year. Most outages were caused by severe weather conditions, such as trees falling due to wind or heavy snow. In Elektrilevi's network, which is the largest distribution grid in Estonia, the average outage time per consumption point per year (SAIDI) caused by failures was 142 minutes in 2024, which was much less than the year before (453 minutes in 2023). Although 2024 was the calmest year in terms of storms in recent years, the functioning of Estonia's distribution grid—especially in rural areas—remains heavily affected by weather conditions.

## THREATS

The main causes of power outages are:

- ✓ Weather phenomena: storms, freezing rain, floods, extreme cold, or extreme heat.
- ✓ Technical causes: human errors; technical failures of critical equipment, including fires.
- ✓ Cyberattacks: targeting power grid control systems or meters, production facilities, and their cloud-based management systems (e.g., power plants, major wind and solar energy providers).
- ✓ Damage to energy infrastructure: theft, sabotage, vandalism, etc.

External connections are critical for the Baltic states. Incidents in the Baltic Sea, such as the destruction of EstLink 2 at Christmas 2024, show that subsea energy infrastructure is vulnerable and has a major impact on society, including electricity prices.

Future crises may be caused by hybrid threats aimed at destabilizing society. Considering the regional geopolitical situation and the full-scale war in Ukraine, it is important to ensure the resilience of critical energy infrastructure against hybrid threats. This requires, among other things:

- ✓ Strengthening physical protection of critical energy infrastructure, taking into account the risks of the new reality (e.g., drones, deliberate damage, sabotage).
- ✓ Ensuring continuous cybersecurity to mitigate risks related to third-party access to energy facilities (e.g., hacking into cloud servers, control systems).

## ACTIONS

- ✓ In 2025, the Baltic states disconnected from the BRELL synchronous grid and joined the Continental European synchronous area. The Baltic energy system is no longer dependent on Russia. Before synchronization, Estonia's electricity system was connected to the synchronous area by six 330 kV high-voltage lines; after synchronization, it is connected by three—these are the links with Latvia. Therefore, Estonia's electricity system must have greater technical capacity to cope with islanding than before.
- ✓ Adequate controllable capacity (e.g., gas and oil shale power plants) in the Baltics, along with cross-border interconnections between member states, help mitigate risks. If the region faces a shortage of generation capacity, for example during an especially long cold period when widespread outages and failures occur simultaneously, electricity consumption may need to be restricted in the worst case. In that situation, electricity would be supplied to consumers on a rotating basis—with outages lasting up to a few hours and announced in advance. Priority would be given to consumers where the risk to human life is highest, such as hospitals and critical nursing homes.

## GUIDELINES

To prepare for a long-term power outage, think through which essential daily activities require electricity and what alternatives you have if electricity is not available:

- ✓ Keep battery-powered lights at home.
- ✓ Have a fully charged power bank for charging your phone.
- ✓ Keep a battery-powered, solar-powered, or hand-crank (dynamo) radio at home to receive official

- ✓ information.
- ✓ Ensure you have enough household supplies to manage independently for one week.
- ✓ If you rely on a public water supply system, ask your local government or water company whether and how water supply is ensured in your area during a power outage.
- ✓ Think about where you could go if you rely heavily on electricity without alternatives. In a long-term outage, you can also receive assistance from your local government.
- ✓ If you have a car, make sure you have enough fuel at home so you can use the radio for information or charge your phone in the car if needed.
- ✓ If possible, acquire a generator and sufficient fuel reserves for it.

#### REPORTING SUSPICIOUS ACTIVITIES

Since hybrid attacks on the power system have a major impact on the functioning of society, it is important to report suspicious activity near power lines or substations **to 112**. Examples include photographing, flying drones, or unusual behaviour.

Handbook Article last update 20.11.2025

## Large-scale communications outage



**Threat assessment:** The realization of a widespread communication outage is likely and is strongly linked to other threats, including power outages, cyber threats, and deliberate human actions. Compared to the previous assessment, the probability of this risk has decreased—from very likely to likely.

A widespread communication outage could disrupt the continuity of other essential services and completely paralyze electronic communications. The seriousness of this threat lies in the fact that people's lives and health could be endangered, and widespread panic could grip society.

The most likely causes of a communication outage are a large-scale power outage, a cyberattack, and/or a failure of physical infrastructure. If these occur simultaneously, they may trigger a widespread communication outage. However, the likelihood of this happening is considered low, provided these events do not occur at the same time in a coordinated and systematic way. This is because telecom operators have preventive and response measures in place for different threats. For example, in the event of a large-scale infrastructure failure, national roaming can be activated. This means that operators can use one another's infrastructure to maintain service continuity.

## THREATS

- ✓ Main sources of risk arise from weather, technology, and the human factor (failures of domestic or international physical infrastructure). Extreme weather conditions can cause widespread power outages, which in turn lead to communication outages. Since communication services rely on various technological solutions, supply chain risks and cyberattacks also pose significant threats.
- ✓ Physical damage to domestic or international infrastructure has been the most common materialized threat in recent years, with potential to affect the continuity of communications. However, in such a case, it would have to involve a clearly large-scale disruption of international connections—single connection failures alone will not cause a communication outage.

## GUIDELINES

Most communication tools used in everyday life depend to some extent on electricity: television, radio, telephone, etc. A widespread power outage may therefore be accompanied by a communication outage. To prepare for such a scenario, you can take preventive measures:

- ✓ Write down the phone numbers of important contacts on paper—if your phone's battery dies, you won't be able to access them.
- ✓ If possible, use the services of multiple telecom operators.
- ✓ Keep a battery-powered radio at home to stay updated with news and official instructions.
- ✓ Keep essential cash at home.
- ✓ Think how you could call for help if necessary.

# Cross-border nuclear accident



**Threat assessment:** The likelihood of a nuclear accident occurring in Estonia's nearby region is low. Compared to the previous assessment, the risk level has not changed.

For Estonia, the greatest potential cause of a nuclear accident would be a serious incident at the closest nuclear power plants (NPPs). These are the Leningrad NPP in the Russian Federation (about 70 km from Narva) and the Loviisa NPP in the Republic of Finland (90 km north of Estonia's coast at Kunda). Under unfavourable weather conditions, radioactive contamination from these plants could be carried through the air to Estonia within a few hours, leading to widespread environmental radioactive contamination and exceeding intervention levels.

The Loviisa NPP in Finland, although about 90 km from Estonia's coastline, does not pose a threat, as its operations and procedures are transparent and reliable. In addition, cooperation with Finnish authorities is ensured. The primary at-risk area in the event of an accident at either the Leningrad or Loviisa NPPs would be Ida-Viru County, but North and Northeastern Estonia would also be affected.

The number of nuclear power plants in neighbouring countries continues to grow. Older reactors are being closed after the commissioning of newer ones, and several new sites are planned (for example, in Poland).



*Nuclear power plants within a radius of 500 km from Estonia*

## THREATS

- ✓ The worst likely scenario is an accident at the Leningrad Nuclear Power Plant in Sosnovy Bor, located about 70 km from Estonia's mainland.
- ✓ Despite advancements in safety standards and technologies, the risks of a nuclear accident will remain for Estonia in the future—the issue lies more in the level and scale of those risks. Even if all old reactors at the Leningrad NPP are closed, new reactors are built, and the issue of storing radioactive waste is resolved, Estonia will still have an obligation, based on IAEA recommendations, to be prepared to mitigate the risks of a nuclear accident.

## ACTIONS

- ✓ A cross-border nuclear accident occurring outside Estonia cannot be brought under Estonia's control. However, the early warning system for radiation hazards serves this purpose by ensuring that the Environmental Board can receive information about a nuclear accident in a neighbouring country at the earliest possible stage.
- ✓ From a radiation safety perspective, nuclear power plants are far enough from Estonia that there is no immediate threat to the lives of Estonian residents.

## GUIDELINES

If you hear or see an official warning about radiation spread, the use of nuclear weapons, or a nuclear power plant accident in a nearby country, then:

- ✓ Take shelter indoors immediately.
- ✓ Follow the instructions provided through official channels.

Handbook Article last update 20.11.2025

# Accident handling industrial hazardous chemicals



**Threat assessment:** The occurrence of a major accident in enterprises handling hazardous chemicals is unlikely. Compared to the previous assessment, the risk level has not changed.

## Map of hazardous and major accident risk enterprises

## Ohtlike ja suurõnnetuse ohuga ettevõtete kaart

In Estonia, there are 66 establishments classified as higher-risk (A and B category) enterprises where various hazardous chemicals are handled. The majority involve the handling of flammable liquid fuels and gases (43.9%), fertilisers (15.2%), the storage of explosives and pyrotechnic products (9%), shale oil

(7.6%), and toxic gases (4.5%). From the perspective of major accidents, the enterprises with the greatest potential impact are generally those located in densely populated areas or in their immediate vicinity.

There is a total of 283 establishments in Estonia categorised as C-level hazardous enterprises. The majority consist of retailers and wholesalers of flammable liquid fuels (petrol stations) and gases (gas installations) (78.5%), ammonia-based cold stores (8.5%), wholesalers of hazardous chemicals (2.5%), galvanic plants (1.4%), and storage facilities for pyrotechnic products and ammunition.

The causes of major accidents in enterprises handling hazardous chemicals include leaks, fires, and explosions. The general underlying reasons are:

- ✓ Human error: violations of various safety requirements, negligence, poor design of buildings or equipment (including protective measures), and design faults.
- ✓ Technological failures: defective equipment, non-functioning of technical protection measures, wear and tear of equipment, failures, and ageing of plant and pipelines.
- ✓ Natural forces: flooding, heavy rainfall, lightning, wind, low or high temperatures, earthquakes/landslides.
- ✓ Accidents caused by interruptions in electricity, heat, water, or communications.
- ✓ Malicious activities: arson, deliberate explosions, and cyberattacks.

## THREATS

- ✓ The proportion of establishments found to have non-compliances has increased over time. In 2024, deficiencies were identified during 84% of site inspections. In the past two years, non-compliances have increased particularly in relation to problems in chemical storage facilities, expired mandatory documentation, shortcomings in fire safety compliance, and insufficient attention to staff training and the conduct of exercises.
- ✓ Extreme weather conditions, such as heatwaves and heavy rainfall, may increase the risk of chemical leaks.

## ACTIONS

- ✓ The Consumer Protection and Technical Regulatory Authority (TTJA), in cooperation with the Rescue Board, has developed and deployed a chemicals module within TTJA's Supervisory Information System (JVIS). Through this module, enterprises handling hazardous chemicals can submit applications for operating permits under the Chemicals Act, as well as mandatory documents for processing and approval. By March 2025, over 57% of all required documents had been submitted through the chemicals module.
- ✓ Technological solutions have helped enterprises reduce the risk of major accidents. For example, smart sensors and artificial intelligence are used to detect and prevent risks. In addition, advanced materials have been introduced which are more durable and safer for storing chemicals. Automation and robotics are also increasingly used in the handling of hazardous chemicals, reducing human exposure.

## GUIDELINES

A chemical accident may be indicated by the activation of sirens in a hazardous or high-risk enterprise, the smell of chemicals, an unexplained feeling of illness, or being in the vicinity of a vehicle involved in an accident bearing hazardous cargo markings.

In the event of a chemical accident:

- ✓ Avoid contact with chemicals.
- ✓ Take shelter indoors.
- ✓ Protect your respiratory system.
- ✓ Follow instructions provided through official channels.

Handbook Article last update 20.11.2025

# Accident with a radiation source



**Threat assessment:** An accident involving a radiation source in Estonia is unlikely. Compared to the previous assessment, the risk level has not changed.

Since Estonia regained independence, more than 35 radiation-related incidents have occurred – an average frequency of 2–3 incidents per year. These have mainly involved the discovery of ownerless radiation sources. Considering the hazards and their likelihood of materialising, there is no reason to believe that such events will become more frequent in the future.

No transport accidents involving the carriage of radioactive substances have been recorded in Estonia. Only one accident has occurred at a production enterprise processing radioactive isotopes during the observed period (in 1994 at a radioactive waste storage facility). Likewise, no significant incidents have been registered in medical institutions. The fall of a satellite or part of one from space is also considered a highly unlikely event.

According to data from the Environmental Board (as of 2024), the following are in use in Estonia:

- ✓ over 1,600 electrical radiation devices (mainly X-ray machines).
- ✓ over 480 devices using sealed radiation sources.
- ✓ over 200 open radiation sources (mainly used in medicine and science).

## THREATS

- ✓ It is not possible to plan exactly for such an event, as an ownerless radioactive container could be discovered during excavation works at any location (including densely populated areas) and at an unforeseen time.
- ✓ A radioactive find could fall into the hands of people who are unaware that it is a radioactive source, or who, even if aware, fail to report it to the authorities. In such cases, ignorance or negligence may endanger their own life and health as well as that of others.

## ACTIONS

- ✓ Regular exercises are held with partner institutions responsible for crisis management, and cooperation is being further developed.
- ✓ There is readiness both to activate a crisis information telephone line and to use EE-ALARM.

## GUIDELINES

If you hear or see an official warning about a radiation hazard, then:

- ✓ Take shelter indoors immediately.
- ✓ Follow instructions provided through official channels.

Handbook Article last update 20.11.2025

# Railway accident



**Threat assessment:** Given that between 6 and 24 railway accidents have occurred annually over the past ten years, the occurrence of a more serious railway accident is considered likely. Compared to the previous assessment, the risk level has not changed.

Most railway accidents take place at level crossings and pedestrian crossings. Railway users are required to give way to trains and must ensure it is safe before crossing the tracks. Unfortunately, fatal accidents occur every year. Over the past decade, the number of accidents has ranged from 6 to 24 annually (excluding suicides). The causes of such accidents may include carelessness, the use of headphones, distraction by mobile phones, as well as being under the influence of alcohol or drugs.

Railway accidents are categorised as either serious accidents or accidents.

- ✓ A serious accident is a train collision or derailment that results in at least one fatality, serious injury to at least five people, or causes serious damage to rolling stock, railway infrastructure, or the environment.
- ✓ An accident is an unplanned or unexpected event, or a chain of events, such as a train colliding with another train or shunting rolling stock, a train striking an obstacle, a derailment, a collision at a level crossing, a person being struck by rolling stock, a fire involving rolling stock, and other such incidents resulting in damage.

## THREATS

- ✓ Planned increases in train speeds to up to 160 km/h may lead to a rise in the number of accidents and an increase in their severity. In recent years, the number of train passengers has steadily grown. Faster train speeds will provide quicker connections between destinations, which could further accelerate passenger growth. Variations in freight volumes may also affect the overall level of safety.
- ✓ Adverse weather conditions may act as a contributing factor. Heavy snowfall, torrential rain, and fog can significantly reduce visibility at crossings. This is particularly dangerous at crossings regulated only by traffic signs. Furthermore, during snowstorms, crossings may not be cleared of snow as required, creating the risk that cars attempting to cross the tracks could become stuck.
- ✓ Rail transport is used to carry large quantities of chemicals. In the event of an accident, this would greatly increase the severity of the consequences.
- ✓ The greatest danger lies in the fact that, under a combination of unfavourable circumstances, a railway accident could become a very serious and high-casualty event. In addition, environmental pollution and/or material damage could result. There is also the risk that a serious accident could occur in a location that requires the use of special equipment to reach those in need of assistance—for example, in forests, fields, bogs, or other areas lacking infrastructure apart from the railway itself. In such cases, providing help would be significantly more difficult.

## ACTIONS

- ✓ To mitigate the risks arising from higher train speeds, the regulations concerning the requirements for level crossings have been updated, and railway infrastructure managers have begun implementing these new requirements. As a result, more grade-separated crossings are being

- ✓ created, and many existing crossings are being upgraded with additional barriers and automatic signal lights.
- ✓ In order to minimise the consequences in the event of an accident, railway accident exercises are carried out.

Handbook Article last update 20.11.2025

## Aviation accident



**Threat assessment:** The occurrence of an aviation accident in Estonia is considered unlikely. Compared to the previous assessment, the risk level has not changed.

Possible causes of an aviation accident may include external environmental threats (fog, strong winds, thunderstorms, heavy rainfall), human activity (the use of an aircraft in a terrorist attack, deliberate damage to equipment, pilot error, or mistakes in air traffic control), as well as the technical condition of aircraft (equipment faults, deterioration, or shortcomings in maintenance).

Estonia is located on the main flight corridor from Asia to Europe, which has always meant a high number of overflights. The full-scale war of aggression launched by Russia against Ukraine in 2022 significantly altered this picture. Essentially, overflights towards Asia by European carriers ceased, leaving only Asia-originating aircraft en route to Europe. As of 2025, the volume of overflights remains 30% lower than before the war.

Air traffic volumes increased again last year: in 2024, Estonia handled 13% more flights than in the previous year, a notable rise. However, compared with the pre-crisis year of 2019, 25% fewer flights were handled. In total, 176,619 flights were managed in Estonian airspace, of which 129,957 were overflights. The number of passengers passing through Estonian airports also grew by about 18% compared with the previous year, exceeding 3.5 million passengers.

## THREATS

- ✓ Reported incidents: In 2024, Lennuliiklusteeninduse AS (Estonian Air Navigation Services) reported 775 incidents. These mainly involved violations of airspace usage permissions, flights over neutral waters without a functioning transponder and without a flight plan, breaches of air traffic controller instructions, and the unauthorised flying of drones in the vicinity of Tallinn.
- ✓ GNSS signal disruptions: The largest number of incidents were related to interference with GNSS signals, occurring within Tallinn's flight information region. While GNSS disruptions do not directly affect overflights, they do impact the work of air traffic controllers and systems, and they may affect the operation of regional airports. These risks can be mitigated with additional systems.
- ✓ Bird strikes: Bird collisions are on the rise, the majority of which occurred at Tallinn Airport. In 2024, a test field was established near the airport to attract birds away from the runway. The test field was mown significantly more frequently than the airport's traffic area, successfully diverting birds away from the runway and reducing the risk of collisions with large birds.

## ACTIONS

- ✓ Compared with 2023, the number of reported incidents increased by around 20%. This rise is due both to the recovery and growth of air traffic after COVID-19 and to an improved reporting culture.
- ✓ The sector must continue to develop and adapt to harness the potential of artificial intelligence, as well as to counter cyberattacks, in order to ensure the resilience of both ground infrastructure and the airborne fleet.

Handbook Article last update 20.11.2025

# Large-scale maritime rescue event



**Threat assessment:** The risk of aviation or maritime rescue incidents in Estonia's search and rescue region is considered unlikely. The probability of a maritime accident is increased by the relatively narrow shipping lane of the Gulf of Finland, intersecting vessel

traffic, and the presence of ice during the winter navigation season. Compared with the previous assessment, the risk level has been raised from very unlikely to unlikely.

Incidents in which a large number of people involved in an aviation or maritime accident require immediate rescue are rare, but they have a significant impact on people, property, and the environment. Responding to such an incident through a large-scale maritime rescue operation requires coordinated cooperation between several countries, different rescue units, and technical resources, with the objectives of saving lives, minimising environmental damage, and ensuring the rapid resolution of the accident. Maritime rescue operations are complicated by the region's dense vessel traffic, severe weather conditions—especially during the winter navigation season—and the need to search for and rescue a large number of people.

In 2024, the Aeronautical and Maritime Rescue Coordination Centre handled 361 rescue incidents, of which 268 took place at sea, 40 on land, and 53 on transboundary water bodies. In recent years, there have been no maritime accidents in Estonian waters requiring assistance for large numbers of people.

#### CAUSES

- ✓ Human factors: fatigue, stress, carelessness, navigational errors, inadequate training, and errors in leadership or decision-making in stressful situations.
- ✓ Machinery, systems, or equipment failures, including hull damage.
- ✓ Weather conditions: fog, strong winds and waves, and winter ice.

#### THREATS

- ✓ The exact number of pleasure craft sailing in the Baltic Sea is unknown due to the free movement between EU Member States.
- ✓ The Gulf of Finland is one of the busiest waterways in the world. The probability of a maritime accident is increased by east–west cargo transport intersecting with the dense ferry traffic between Helsinki and Tallinn.
- ✓ Every year, incidents occur involving large groups of fishermen venturing onto the ice (mainly on Lake Peipus, Lake Pskov, Lake Lämmijärv, and Pärnu Bay) in defiance of ice bans and despite

- ✓ adverse weather conditions. The main risk group consists of recreational fishermen, who generally neither recognise nor understand the dangers they face while on the ice. In most cases, those in need of assistance are recreational fishermen and amateur seafarers.
- ✓ The accumulation of vessels awaiting access to port in a confined area near the fairway.
- ✓ The rapid growth of the maritime economy, including the construction of offshore wind farms.
- ✓ The activities of the Russian Federation.

#### ACTIONS

- ✓ The large-scale maritime rescue operation plan creates the conditions for better-prepared cooperation, smoother coordination, and the effective deployment of international assistance.
- ✓ The use of drones is developing rapidly for a variety of tasks, including aviation and maritime rescue. Rescue drones can help to quickly identify accident locations, deliver rescue equipment, and monitor the situation on-site in real time.
- ✓ The development of smart buoys makes it possible to obtain accurate real-time information on wind conditions, wave height, currents, and water temperature in a given area. This supports aviation and maritime rescue operations and provides increasingly precise data on weather conditions, helping to prevent accidents. The adoption of new technologies also brings with it the need to further develop the knowledge and competencies of specialists working in the field of maritime and aviation rescue.

Handbook Article last update 20.11.2025

## Large-scale marine pollution



**Threat assessment:** The risk of marine pollution occurring in Estonian waters is

considered likely, taking into account the intensity of international shipping traffic. Increasing cargo transport, the region's complex navigational conditions, and vessels belonging to Russia's shadow fleet all raise the probability of this risk materialising.

Marine pollution is a significant threat in Estonian waters and may arise from multiple sources: the transport of oil products and chemicals, ship collisions, leaking wrecks, port activities, and the development of offshore wind farms. Pollution can damage marine ecosystems and wildlife and threaten human health as well as economic activity.

Several minor pollution incidents have occurred in Estonian waters in previous years, some linked to port activities and others to fuel leaks from vessels. Officially recorded large-scale incidents have been few, but the environmental impact of earlier cases has been considerable. In recent years, however, the risk of potential tanker accidents has increased.

#### THREATS

- ✓ Large, busy, and unregulated anchorage areas have formed near Naissaar and Vaindloo islands for cargo ships waiting for access to loading facilities, mainly in Russian ports.
- ✓ An increasing number of tankers sail in Estonian waters, not all of which comply with international maritime safety conventions.
- ✓ More than 600 shipwrecks have been identified in Estonian waters. Of these, around 60 are considered to pose a significant environmental hazard due to the quantity and danger of oil products in their tanks. A large share of these wrecks date back to the First and Second World Wars.

#### ACTIONS

- ✓ National and international exercises have simulated pollution scenarios, which have demonstrated that pollution response preparedness and coordination require continuous improvement.
- ✓ Within the framework of the international AISRISK II project, work is under way to adapt a dynamic risk assessment tool to Estonian conditions, enabling more precise monitoring and evaluation of pollution risk dynamics. Plans also exist to use the

- ✓ EcoSensitivity Tool for scenario-based impact analysis in cooperation with the University of Tartu's Estonian Marine Institute.
- ✓ A national marine pollution response concept is under development. This will define responsibilities and develop cooperation mechanisms.

## GUIDELINES

If you notice oil-contaminated birds, environmental pollution, or the threat of pollution, report this by calling the national information hotline 1247. Reports can also be sent by email to [1247@1247.ee](mailto:1247@1247.ee)

If you discover or cause marine pollution, notify the following contacts as soon as possible:

Aeronautical and Maritime Rescue Coordination Centre (JRCC Tallinn): +372 619 1224

Radio Frequencies:

- VHF-DSC Channel 70
- VHF Channel 16
- VHF Channel 69
- MF-DSC 2187.5 kHz
- 2182 kHz

Radio Call Signs:

- On VHF Channels 16 and 69, call TALLINN MEREVALVEKESKUS (in English: Tallinn RESCUE).

Handbook Article last update 20.11.2025

# Explosion



**Threat assessment:** A large-calibre ammunition explosion with human casualties is considered likely. Domestically, the risk is unlikely, but considering the war in Ukraine and the lessons drawn from it, the danger may originate from outside Estonia. In the future, situations may arise in which explosives used in Ukraine are smuggled across the border and employed for criminal purposes. Compared with the previous assessment, the likelihood of this risk has increased from unlikely to likely.

Finds of ammunition are mainly connected to the battles of the Second World War, with the highest number of calls typically occurring in four counties: Harju, Ida-Viru, Saare, and Tartu. However, explosive devices may be encountered anywhere across Estonia. Even today, relatively large quantities of wartime ammunition continue to be found on Estonian territory. Excavation or agricultural work, as well as natural landslides, may expose dangerous items. Abandoned wartime and modern ammunition may also be discovered, and handling such material can create an explosion hazard. Construction and forestry activities increase the likelihood of contact with ammunition. Each year, bomb disposal specialists render safe a substantial number of explosive devices:

- 2020: 9,041
- 2021: 6,930

- 2022: 14,985
- 2023: 10,840
- 2024: 6,622

Although the number of explosions caused by explosives in Estonia has fallen significantly compared with the 1990s, it has not dropped to zero. The primary reason is the continued illegal handling of explosives.

## THREATS

- ✓ It is easy to obtain information from the internet on how to manufacture explosives. In addition to homemade explosives, materials are also sourced from discovered ammunition.
- ✓ Since the Russian Federation's war of aggression against Ukraine began in 2022, the movement of explosives across Europe has increased, along with the risk of hostilities mistakenly spreading beyond national borders.
- ✓ Over time, explosives may become even more dangerous, as protective mechanisms weaken with age, while the explosive material itself does not lose its properties and may become more sensitive.

## ACTIONS

Public awareness and involvement are promoted through the Rescue Board's communication and prevention activities, planned bomb disposal operations, various handover campaigns, travelling exhibitions, and the engagement of volunteers. The risks of explosions are mitigated by carrying out bomb disposal work and raising public awareness.

## GUIDELINES

In the event of an explosion hazard:

- ✓ Report the danger or discovery immediately to the Emergency Response Centre by calling 112.
- ✓ Do not touch or move the explosive object; retreat at least 50 metres away from it.
- ✓ Stay behind a building or structure and keep away from windows.
- ✓ Follow official instructions and be prepared for evacuation.

Handbook Article last update 20.11.2025

# Building fire



**Threat assessment:** A fire resulting in a large number of casualties is considered unlikely. Compared with the previous assessment, the risk level has not changed.

Building fires can have severe consequences for human life, property, and the functioning of society. Fires are especially dangerous in buildings where many people are present, such as care homes, hospitals, or assembly buildings. Evacuation is made more difficult if people are unfamiliar with the building layout or require assistance, for example due to physical or mental disabilities. Although such

institutions have trained staff, the rapid spread of fire and the onset of panic can make evacuation complex. If exits are blocked by smoke, flames, or structural collapse, the risk of fatalities increases. Smoke and toxic gases are the main causes of death in building fires.

Fires in industrial buildings and warehouses can destroy critical infrastructure and cause extensive property damage. If chemicals or hazardous substances ignite in densely populated areas, toxic smoke may be released, endangering large numbers of people and potentially requiring large-scale evacuation. In addition to the immediate risks to life and property, such an incident may cause long-term health hazards and necessitate continuous monitoring of air and water quality. Extinguishing operations may also lead to environmental pollution, for example through contaminated firefighting water and hazardous waste, which can spread beyond the immediate fire zone.

In recent years, the number of building fires has declined. Over the past five years, there has also been a downward trend in the number of injuries, although the number of fatalities has remained relatively stable. Fires in residential buildings make up the majority of all building fires. Although the number of residential building fires has decreased over time, the probability of a fire remains high—around 1.5 residential fires occurred per day in 2024. In other types of buildings, there was an average of 0.5 fires per day in 2024.

## THREATS

- ✓ The number of fires may rise due to the global trend of increasing fires caused by lithium-ion batteries, which has not yet fully reached Estonia. Lithium-ion batteries are highly flammable, particularly when damaged, overloaded, or improperly maintained. A short circuit or overheating inside a battery may cause thermal runaway, leading to overheating and explosion. Such an event can result in an intense fire, as lithium-ion batteries can burn at extremely high temperatures and even explode.
- ✓ Between 2017 and 2024, the main causes of residential building fires were electrical installation and appliance failures, as well as negligent use of electrical equipment (26%), heating systems (23%), and smoking (14%). A significant share of fires is caused by human activity.
- ✓ In 2024, 3,879 non-residential buildings (industrial, accommodation, public, and other types) were inspected, and fire safety deficiencies were identified in 69% of cases. The majority were assembly buildings: shopping centres, care institutions, catering establishments, restaurants, theatres, cinemas, primary schools, universities and other research institutions, libraries, clubs, etc. According to fire safety inspections carried out between 2021 and 2024, the main deficiencies were related to emergency lighting (17%), fire alarm systems (16%), fire compartment integrity (13%), exits and evacuation routes (11%), other fire safety installations (9–10%), and procedures in case of fire (8%).

## GUIDELINES

A fire in a building must be reported immediately by calling the emergency number 112.

- ✓ Leave the burning building at once.
- ✓ Protect yourself from fire and smoke.
- ✓ If you cannot exit the building, make your presence known.
- ✓ Help others, but do not endanger your own life or health.

Handbook Article last update 20.11.2025

# Collapse



**Threat assessment:** Large-scale collapses of apartment buildings or mines are considered unlikely. Compared with the previous assessment, the risk level has not changed.

The causes of collapses can be broadly divided as follows:

- ✓ Design or construction errors: mistakes made during the planning or construction of buildings, illegal alterations, misuse of the structure, poor maintenance, or structural ageing.
- ✓ Natural forces: for example, excessive snow loads or soil washed away by erosion.
- ✓ Underground mining: collapses or subsidence of mine workings and shafts may cause ground deformations or deep sinkholes, leading to structural damage to buildings on the surface.

## THREATS

The main problems affecting buildings are:

- ✓ Cracks or failures of load-bearing structures caused by foundation subsidence.
- ✓ Poor technical condition and deterioration of building structures.
- ✓ Poor technical condition of balconies in panel buildings.
- ✓ Illegal extensions or removal of load-bearing structures.
- ✓ Buildings rendered unsafe due to fire or traffic accidents.

## ACTIONS

- ✓ The Environmental Board receives an average of 2–3 reports per year of mining-related sinkholes. By the beginning of 2024, there were 10 sinkholes known to be awaiting safety measures and remediation.
- ✓ Through the Land Board and Spatial Data Agency's geoportal, it is possible to access the mineral deposits mapping application, which provides information on areas undermined by oil shale mining, preserved structures left during underground mining, and the locations of mine shafts.

## GUIDELINES

Warning signs of collapse risk include explosions, subsidence of building structures, or the rapid cracking and breaking of walls, ceilings, or floors.

If you are unable to exit a collapsing building:

- ✓ Stay calm.
- ✓ Protect your airways from dust.
- ✓ Call 112 if possible.
- ✓ Move slowly and cautiously.
- ✓ Signal your presence, but conserve your strength.

Handbook Article last update 20.11.2025

## CBRN incident



**Threat assessment:** The probability of an incident in Estonia caused by the malicious or

terrorist use of chemical, biological, radiological or nuclear (CBRN) materials within the next five years is considered low. However, technological development and the wider use of drones may increase the likelihood of such an attack in the longer term, as the necessary expertise and equipment are becoming more easily accessible.

Both terrorist groups and radicalised individuals have attempted to carry out attacks in the EU with large numbers of casualties, aiming to exert psychological and economic pressure on society and political decision-making. Terrorist organisations have not yet used CBRN materials in attacks in Europe, but preparations for this have been made. These organisations are intent on acquiring chemical, biological, radiological, and nuclear materials or weapons and are seeking to develop the capability to obtain and use them. Attacks by radicalised lone actors influenced by extremist ideologies also cannot be excluded.

In addition to terrorist organisations, CBRN-related attacks may also be associated with hostile foreign states. CBRN materials have been used in military conflict zones, including in Ukraine, for carrying out attacks. In situations of armed conflict, there is always the possibility that weapons of mass destruction could fall into the hands of terrorist or extremist groups.

In Estonia, CBRN-related incidents have so far been linked to smuggling cases involving CBRN materials for the purpose of criminal profit.

Although rare, incidents involving CBRN materials can have extremely severe consequences. Beyond their immediate effects at the site of the incident, such events may cause uncertainty and panic within society, lead to the spread of misinformation in mass media and social media, and damage the country's reputation.

## THREATS

- ✓ According to the International Atomic Energy Agency's (IAEA) Incident and Trafficking Database (ITDB), as of 2024, there have been 147 incidents worldwide involving radiation sources or nuclear material. The occurrence of incidents involving radiation sources cannot be ruled out in the Estonian context either.
- ✓ In Estonia, the risk of theft of radiation sources is currently low, and storage facilities for radiation sources apply additional security measures.
- ✓ As of 2024, there are 68 major accident hazard and dangerous enterprises in Estonia where large

- ✓ quantities of hazardous chemicals are handled. The likelihood of attacks on chemical storage sites in Estonia is currently low.
- ✓ There are states and terrorist groups exploiting advances in biology, including microbiology and genetic engineering, to develop weapons of mass destruction. In Estonia too, it cannot be ruled out that individuals influenced by extremist ideologies might use toxins (such as ricin) to carry out an attack.

Handbook Article last update 20.11.2025

## Previously assessed risks

Here you will find risks whose probability was last assessed before 2025.

Handbook Article last update 20.11.2025

## Organised crime



Risk assessment (assessed 2024): The trend of organised crime posing a threat to national security remains stable. There is an increased probability of the illegal proliferation of weapons of mass destruction and strategic goods.

### CAUSES

Organised crime networks are particularly active in cross-border drug, cyber, economic, and

environmental crime, as well as human trafficking, the provision of criminal services, and support for terrorism. There is an increasing shift towards white-collar crime (e.g. fraud). Organised crime networks are flexible, evolving, and adapting, while avoiding being investigated by law enforcement.

- ✓ Two thirds of serious and organised crime offenders in Europe are regularly involved in corrupt activities. More than 80% of criminal networks use legitimate business structures.
- ✓ Around 60% of criminal networks operating in the EU use violence in their criminal activities. Violent crime has become more common in Europe.
- ✓ Around 40% of criminal networks operating in the EU are linked to illicit drug trafficking, which remains a major source of income. Drug trafficking is also one of the main sources of income for organised crime in Estonia.
- ✓ The line between cybercrime and other crime is blurring. Virtual cyberspace is being exploited to commit so-called classic crimes such as fraud, selling drugs, and more.
- ✓ Although organised crime maintains a low profile in Estonia, random and spontaneous violent crimes are still committed. Proceeds are also earned from economic crime, human trafficking, and theft.

## THREATS

- ✓ The level of organised crime in Estonia has remained relatively low. A future threat is the possible expansion of international criminal networks into Estonia.
- ✓ The classic organisational cultures of organised crime are being replaced, including in Estonia, by modern criminal associations developing flexible management styles. With this change comes the risk that criminal activity will become more effective and harder to deter, leading to increased financial losses.
- ✓ Organised criminals are increasingly moving into cyberspace. This carries the risk that more and more vulnerable groups in society, with below average digital literacy, will become victims.
- ✓ Due to the war in Ukraine, weapons and ammunition may also fall into the hands of Estonian criminal groups, which could threaten the security of society.
- ✓ The biggest negative impact of organised crime on society comes from drug trafficking, which is the biggest source of income for criminal organisations and continues to pose a threat to public health.
- ✓ Due to our proximity to Russia, which has a high level of organised crime, we also must consider

- ✓ potential impacts from the east. The special services of the Russian Federation use criminals and organised crime to gather cross-border intelligence, undermine the target state, and given the chance, stage a coup.

Expand all

[Read more](#)

[Prosecutor's Office Yearbooks](#)

European Council: <https://www.consilium.europa.eu/en/policies/eu-fight-against-crime/> opens in a new tab

INTERPOL: <https://www.interpol.int/Crimes/Organized-crime> opens in a new tab

Handbook Article last update 20.11.2025

## Transport accident on the road



**Risk assessment (assessed 2024): The probability of a major accident (ten or more victims) is low.** The risk assessment has not changed compared to the previous risk analysis.

According to the Estonian Motor Insurance Bureau, there were 34,314 motor insurance cases in Estonia in 2023, of which 1,724 (1.5% more than in the previous year) were traffic accidents with injuries or fatalities. The increase is mainly due to an increase in the number of accidents involving personal light electric vehicles. Harju County, including the city of Tallinn, stands out with the highest number of accidents.

Major accidents (ten or more victims) account for less than 0.01% of the total number of accidents. There was a total of six such accidents between 2017 and 2023.

According to statistics, 26% of people injured in transport accidents were in a serious condition and required hospital treatment for more than 24 hours. The rest did not need prolonged treatment.

#### CAUSES AND THREATS

- ✓ **human factor**, including negligence, disregard of safety rules, or violation of traffic laws.
- ✓ **technical factors**, including the use of technically unsound means of transport or unforeseen technical breakdowns.
- ✓ severe or unexpected changes in **weather conditions**, increase in extreme weather events.
- ✓ continued growth in mileage.
- ✓ **self-driving cars on the road** (events caused by failures of navigation systems).
- ✓ **intelligent transport systems** (ITS) can be exploited in the future to carry out cyber-attacks or attack the systems themselves.

#### WORST-CASE SCENARIO

**A high-speed collision between two buses.**

#### CODE OF CONDUCT

If you are involved in an accident, or see an accident with people injured, call 112 immediately. As calmly as possible, say what has happened, what you see, where the accident happened, and answer all the questions asked by the rescue officer.

You can find comprehensive instructions on how to act in the event of a road accident on the website of the Estonian Rescue Board: [traffic accident opens in a new tab](#)

Expand all

[Read more](#)

[Statistics on road accidents in Estonia opens in a new tab](#) Estonian Transport Administration

## Marine casualty



**Risk assessment\*:** The likelihood of a marine casualty in Estonian waters with a high number of casualties or significant environmental damage is low. Compared to the previous assessment, the risk likelihood has been raised from unlikely to low.

*\*In 2025, the risk of marine casualty was not assessed, but the threat of a large-scale maritime rescue event and a large-scale marine pollution were assessed separately*

Marine casualties are usually caused by **human error**. In recent years, the number of vessels in distress has been on an upward trend, but this is mainly due to the increase in the number of recreational craft. In 2023, there were fifteen officially recorded incidents (10) or casualties (5) in Estonian waters and a total of 29 cases were recorded. The most notable of these were the unsafe approach of two vessels, R/L Elina and R/L Baltic Queen; the listing of R/L Amalie, which required the evacuation of passengers, and the collision of R/L Regula with a quay.

### CAUSES AND THREATS

- ✓ Nearly 90% of marine casualties are caused **by human error**: navigation error, miscalculation, sudden manoeuvres, inadequate or incorrect assessment of hazards, inattention or distraction, misunderstandings, etc.
- ✓ **Technological causes**: failure of machinery, systems, or equipment, hull damage.
- ✓ **Adverse weather conditions**.

### FACTORS INCREASING THE RISK

- ✓ **dense and intersecting** vessel traffic and **increasing traffic of recreational craft**.

- ✓ **growth in liquefied natural gas (LNG) shipments.**
- ✓ **expansion of offshore wind farm areas.**
- ✓ **trends in maritime technology**, including the use of novel, untested ship control and navigation tools in narrow and congested lanes.
- ✓ **activities of the Russian Federation.**
- ✓ **undetected movements of vessels** (AIS transmitter deactivation, GPS manipulation, etc.).
- ✓ Bunkering in more economically viable but more exposed areas, as well as fuel leaking from wrecks that have sunk decades ago (it is estimated that there are 57 environmentally hazardous wrecks in Estonian waters) **increase the risk of pollution.**

#### WORST-CASE SCENARIO

**A collision between a passenger ship and an oil tanker in the Estonian rescue area.**

#### CODE OF CONDUCT

If you are involved in an accident or see an accident with casualties, please report it immediately to the Joint Rescue Coordination Centre (JRCC Tallinn) of the Police and Border Guard Board by calling 619 1224 or 112. As calmly as possible, say what has happened, what you see, where the accident happened, and answer all the questions asked by the rescue officer. As a passenger on a ship:

- ✓ check the locations of the assembly points and lifesaving equipment at the start of the trip.
- ✓ in case of an emergency, follow the instructions of the staff and authorities.
- ✓ go to the nearest assembly point when instructed to do so.
- ✓ take only essential items with you:

- documents and phone.

- the everyday medicines you use.

- wear warm clothes.

- ✓ Stay on board as long as possible, avoid getting into the water.

Stay calm and follow the instructions of the authorities and the emergency services.

Expand all

**Read more**

**Statistics on marine casualties opens in a new tab**, Estonian Transport Administration

**Annual Overview of Marine Casualties opens in a new tab**, Europe Maritime Safety Agency (EMSA).

Reviews of the **Baltic Marine Environment Protection Commission opens in a new tab** (HELCOM)

**Website of the ferry M/S Estonia opens in a new tab**, Safety Investigation Bureau

Handbook Article last update 20.11.2025