SISEKAITSEAKADEEMIA
Estonian Academy of Security Sciences
INTERNAL SECURITY INSTITUTE

EMILIA MUUGA, RAUL SAVIMAA, JAANIKA PUUSALU,
RAMON LOIK, RINGO RINGVEE, MÄRT LÄÄNEMETS,
JÜRI SAAR, GEORG-HENRI KAUP

FORECAST OF GLOBAL TRENDS AFFECTING ESTONIA'S INTERNAL SECURITY

2026–2030

Co-funded by the European Union
Republic of Estonia
Ministry of the Interior

EMILIA MUUGA, RAUL SAVIMAA, JAANIKA PUUSALU,
RAMON LOIK, RINGO RINGVEE, MÄRT LÄÄNEMETS,
JÜRI SAAR, GEORG-HENRI KAUP

Forecast of global trends affecting Estonia's internal security 2026–2030

The authors thank Jüri Vlassov and Mari-Liis Tori for reviewing the manuscript and for their valuable comments.

Cover image: Microsoft Copilot, 2025

Layout and design: Jan Garshnek

Translation and copy-editing: Refiner Translations OÜ

Print: Paar

ISBN 978-9985-67-540-3 (print)

ISBN 978-9985-67-541-0 (pdf)

DOI: https://doi.org/10.15158/h2nt-y802

www.sisekaitse.ee

TABLE OF CONTENTS

FOREWORD

For years, countries around the world have had to adapt to a turbulent era characterised by multiple crises[1] and a wide range of other challenges. Uncertainty and anxiety in society are rising. In addition to the actions of Russia and China, the unpredictability of US foreign and security policy has become an increasing concern, as has the uncertainty over whether there is sufficient consensus and strength within the European Union and NATO to preserve stability.

For Estonia, Russia – and the potential deterioration of the overall security environment that follows from its behaviour – remains the principal security threat. Although the risk of a conventional attack against Estonia exists, the Estonian Foreign Intelligence Service (Välisluureamet, 2025) has determined the level of threat to be low for now. Nevertheless, one should treat the mitigation of that risk with the utmost seriousness and consider it necessary to prepare for the worst. In this regard, Estonia's security undoubtedly depends on the ongoing developments in Ukraine. However, it is clear that threats to Estonia's internal security do not arise solely from Russian activity, and, alongside coping with protracted crises and mitigating heightened military risks, Estonia should also proactively prevent other types of threats.

As states face an unprecedented flood of information and the uncertain consequences of integrating artificial intelligence into everyday life, it is increasingly important to strengthen our population's knowledge, critical-thinking skills and ability to recognise manipulation. The spread of misinformation and disinformation constitutes one of the most consequential risks for Estonia, so it is essential to address the distinct, contemporaneous vulnerabilities that authoritarian-leaning states skilfully exploit to target and manipulate audiences with propaganda on social media and digital platforms. The manipulation and spread of falsehoods that accompany political parties' domestic struggles for power also feed societal polarisation and radicalisation from within. This inevitably raises a wider question: if a state uses such techniques on its own society, does that thereby undermine its capacity to protect the public from large-scale influence operations conducted by external actors?

A broad approach to national defence that addresses multiple threat vectors is the key to prevention, as well as to preparing society to cope should several threats materialise simultaneously. As crises persist, the state must maintain rapid development and response capacities and the ability to integrate emerging technologies successfully into preparedness and defensive capabilities, rather than allowing technologies to evolve only

[1] In this report, *multi-crisis* denotes the simultaneous occurrence of several different crises affecting society. These events need not be directly related, nor must their mutual effects necessarily reinforce one another. They have different causes and cannot be solved by a single uniform measure.

as tools used against those capacities. Beyond Russia, which tends to pursue its objectives loudly, Estonia is faced with various latent but nonetheless purposeful risk factors. None of the most widely cited risk assessments from only a short period of time ago foresaw that, within a couple of years, the greatest threats would be a global pandemic and military activity in Europe. Estonia must learn from that and prepare for threats that, for now, may not yet be knocking at the door.

The aim of this five-year (2026–2030) forecast of global trends affecting Estonia's internal security is to provide evidence-based strategic input for the development of Estonia's security policy, including the framework document *National Security Concept of Estonia* (*Eesti julgeolekupoliitika alused*). To that end, the Research Centre of the Internal Security Institute at the Estonian Academy of Security Sciences conducted a study in early 2025 with the assistance of 24 Estonian subject-matter experts in which 29 global risks rated most likely to materialise internationally were assessed for their potential impact on Estonia. In assessing these risks and their impacts, the study focused on a medium-term horizon (5–7 years) and ranked them by the likelihood of their occurrence and by the potential magnitude of their effect on Estonia. Researchers at the Estonian Academy of Security Sciences added analysis and explanations.

GLOBAL RISK ASSESSMENTS

The World Economic Forum (2025) and the European University Institute (Anghel, 2025) have determined the spread of misinformation and disinformation, the occurrence of interstate armed conflicts, the conclusion of a ceasefire favourable to Russia in the war with Ukraine, and a US withdrawal from security guarantees offered to European allies to be among the most likely and highest-impact global risks for Europe and the world as of 2025 and in the coming years (see a more detailed description of the risks in Appendix 2).

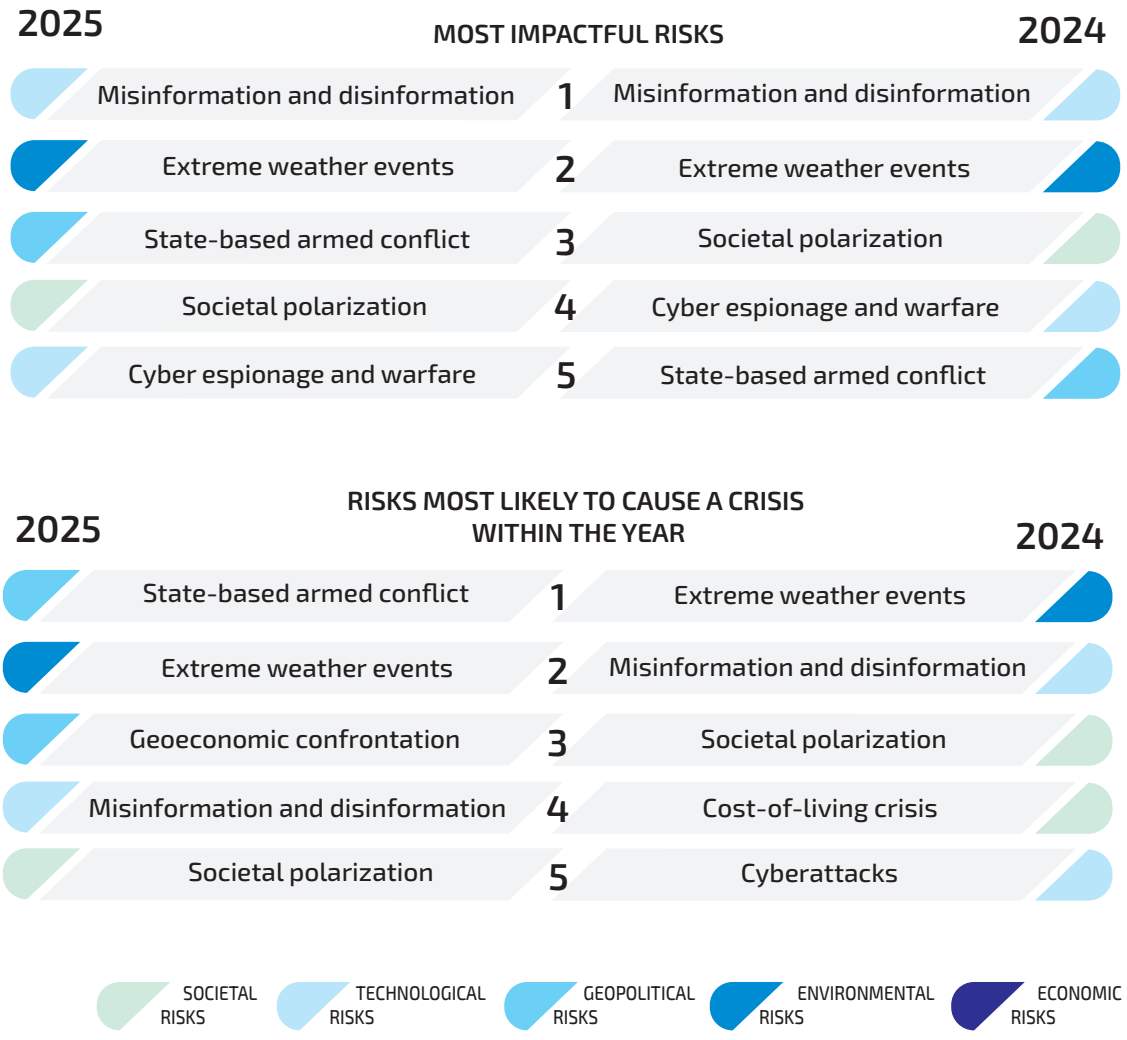

FIGURE 1. COMPARISON OF WORLD ECONOMIC FORUM RISK ASSESSMENTS FROM 2024 AND 2025 (SOURCE: WORLD ECONOMIC FORUM)

According to the World Economic Forum's Global Risks Perception Survey (World Economic Forum, 2024, 2025), the spread of misinformation and disinformation was judged the single most impactful risk over a two-year horizon in both 2024 and 2025. In second place for both years were events caused by extreme weather. Whereas the 2024 report ranked social polarisation as the third most significant risk, in 2025 that position was occupied by the risk of interstate armed conflict. (See Figure 1). By comparison, in 2019 and 2007 the most impactful risks were judged to be the use of weapons of mass destruction and the bursting of an asset-price bubble (World Economic Forum, 2020).

In a shift from the previous year's report, the 2025 report finds interstate armed conflict most likely to cause a crisis within the year. For comparison, risks such as extreme weather and infrastructure disruptions were assessed as among the most impactful in the reports from 2007 and 2019 (World Economic Forum, 2020). Over a ten-year horizon, on the other hand, the top four highest-impact risks listed in both the 2024 and 2025 reports were all environmental in nature (see figure 2).

The World Economic Forum report also includes the results of a leaders' survey to identify the risks that each country's respondents judged most likely to pose the greatest threat over the next two years. In the 2025 report, the respondents from Estonia and Latvia ranked the risk of military conflict highest, followed by the risk of economic downturn. In the previous year's report, economic downturn was viewed as the single greatest risk for Estonia (see Figure 3).

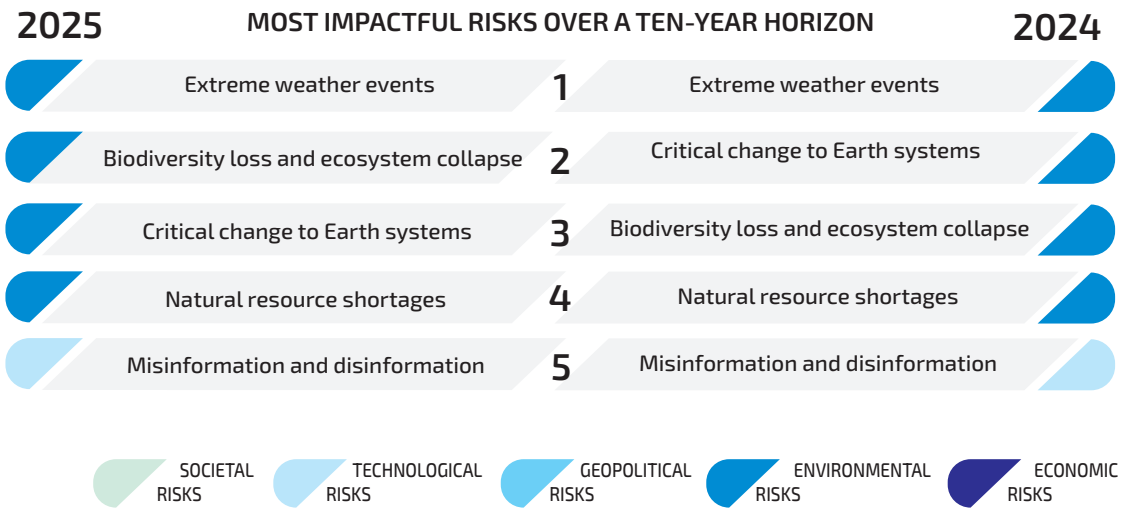

FIGURE 2. COMPARISON OF WORLD ECONOMIC FORUM RISK ASSESSMENTS WITH A TEN-YEAR HORIZON FROM 2024 AND 2025 (SOURCE: WORLD ECONOMIC FORUM)

FIGURE 3. COMPARISON OF WORLD ECONOMIC FORUM LEADERS SURVEYS FROM 2024 AND 2025 FOR ESTONIA, FINLAND AND LATVIA (SOURCE: WORLD ECONOMIC FORUM)

According to the study ***Global risks for the EU*** (Anghel, 2025), the highest-impact risks for the EU are the possible US withdrawal of security guarantees for European allies and hybrid attacks on the EU's vital infrastructure. The risks rated most likely to materialise were the failure to achieve a ceasefire between Israel and Hamas and the accession of a pro-Russia government in Georgia (see Figure 4).

FIGURE 4. GLOBAL RISKS WITH THE HIGHEST IMPACT ON EUROPE (SOURCE: ANGHEL, 2025)

In the Estonian Academy of Security Sciences' expert survey conducted in early 2025, the global risks rated most likely to materialise were the spread of misinformation and disinformation and geoeconomic confrontation (see Figure 5). Other risks considered highly likely were interstate armed conflict, social polarisation, and cyber espionage and warfare. Although environmental risks were assessed as having only medium probability over a 5–7-year horizon, experts rated them substantially more likely over a 10–50-year horizon.

LIKELIHOOD OF THE MATERIALISATION OF GLOBAL RISKS OVER A 5–7-YEAR HORIZON

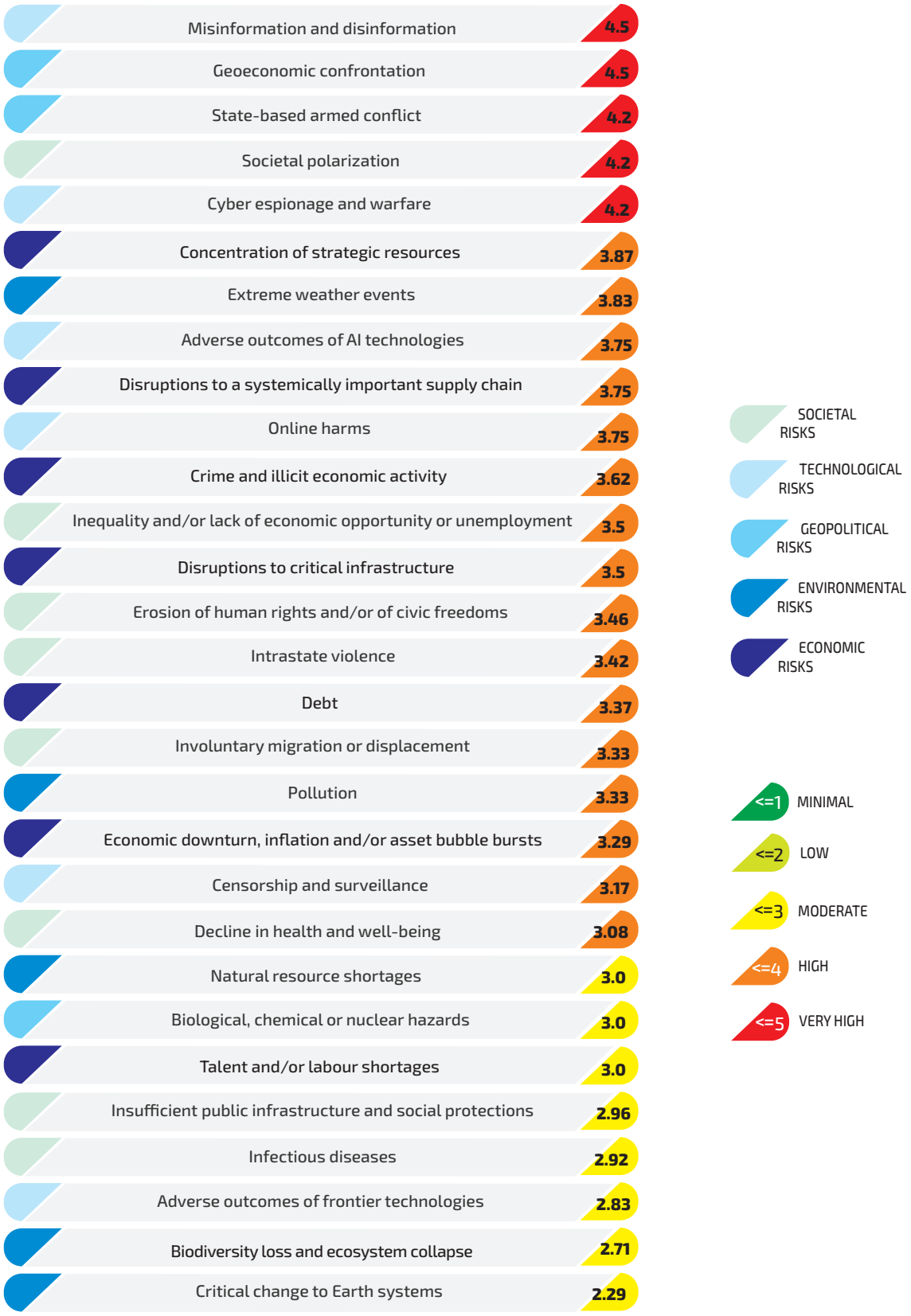

FIGURE 5. ESTONIAN EXPERTS' ASSESSMENTS OF THE LIKELIHOOD OF THE MATERIALISATION OF GLOBAL RISKS

The following section outlines the potential impacts of the five risks rated most likely to affect Estonia.

THREATS MOST LIKELY TO AFFECT ESTONIA

In spring 2025, Estonian experts were asked to assess (see Appendix 1) individually the likelihood of each global risk materialising and the potential impact on Estonia should it do so. In a combined view of the two criteria (highest likelihood of occurrence and greatest impact on Estonia), the top risks were judged to be cyber espionage and warfare and the spread of misinformation and disinformation (Figure 6).

In addition to cyber espionage and warfare, and misinformation and disinformation, experts determined interstate armed conflict, geoeconomic confrontation and social polarisation to be among the risks likely to have the greatest impact on Estonia (Figure 7). Experts rated environmental risks as only a medium probability over a 5–7-year horizon but substantially more likely over a 10–50-year horizon.

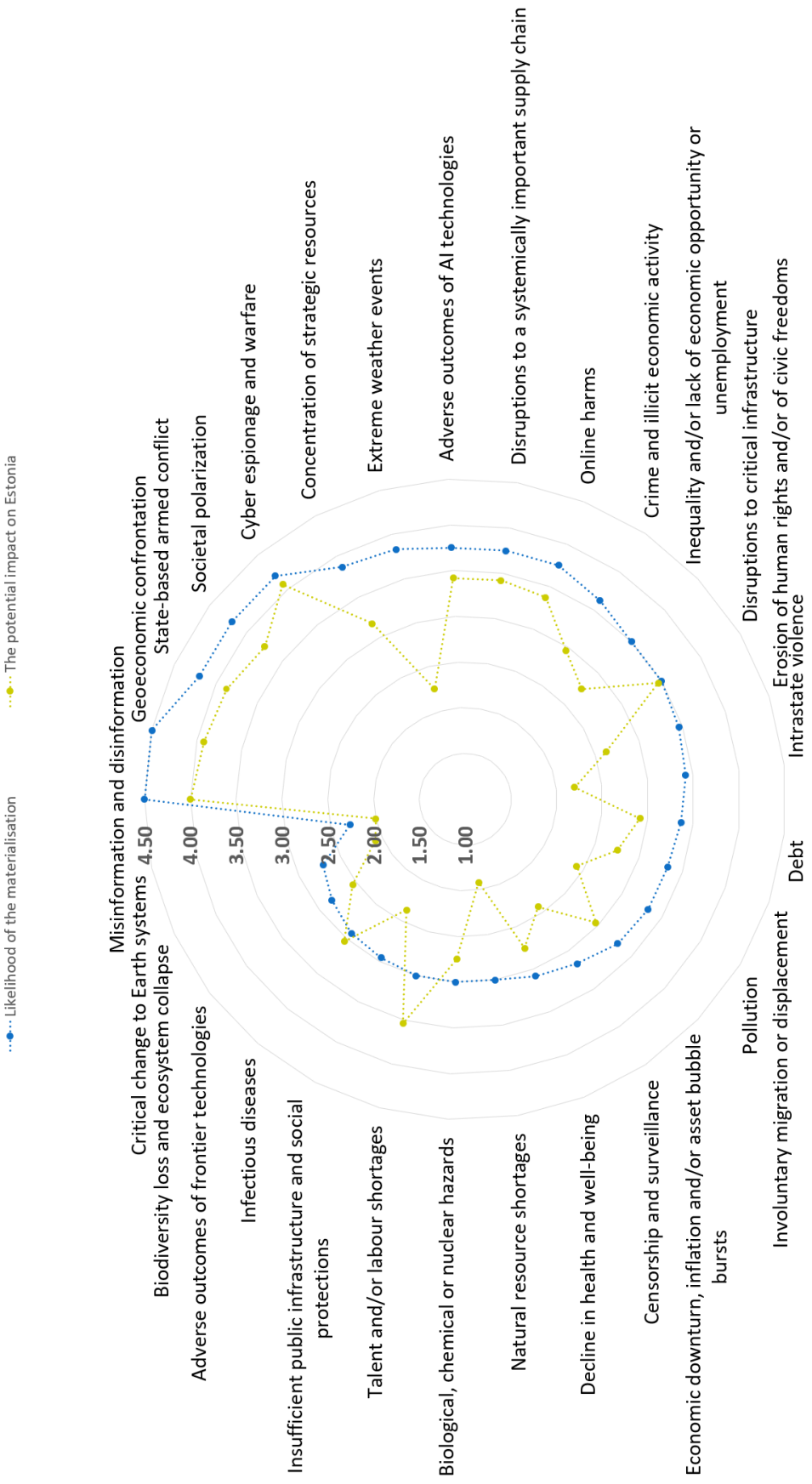

FIGURE 6. ESTONIAN EXPERTS' ASSESSMENTS OF THE LIKELIHOOD AND POTENTIAL IMPACT OF GLOBAL RISKS FOR ESTONIA

RISKS WITH THE GREATEST POTENTIAL IMPACT ON ESTONIA

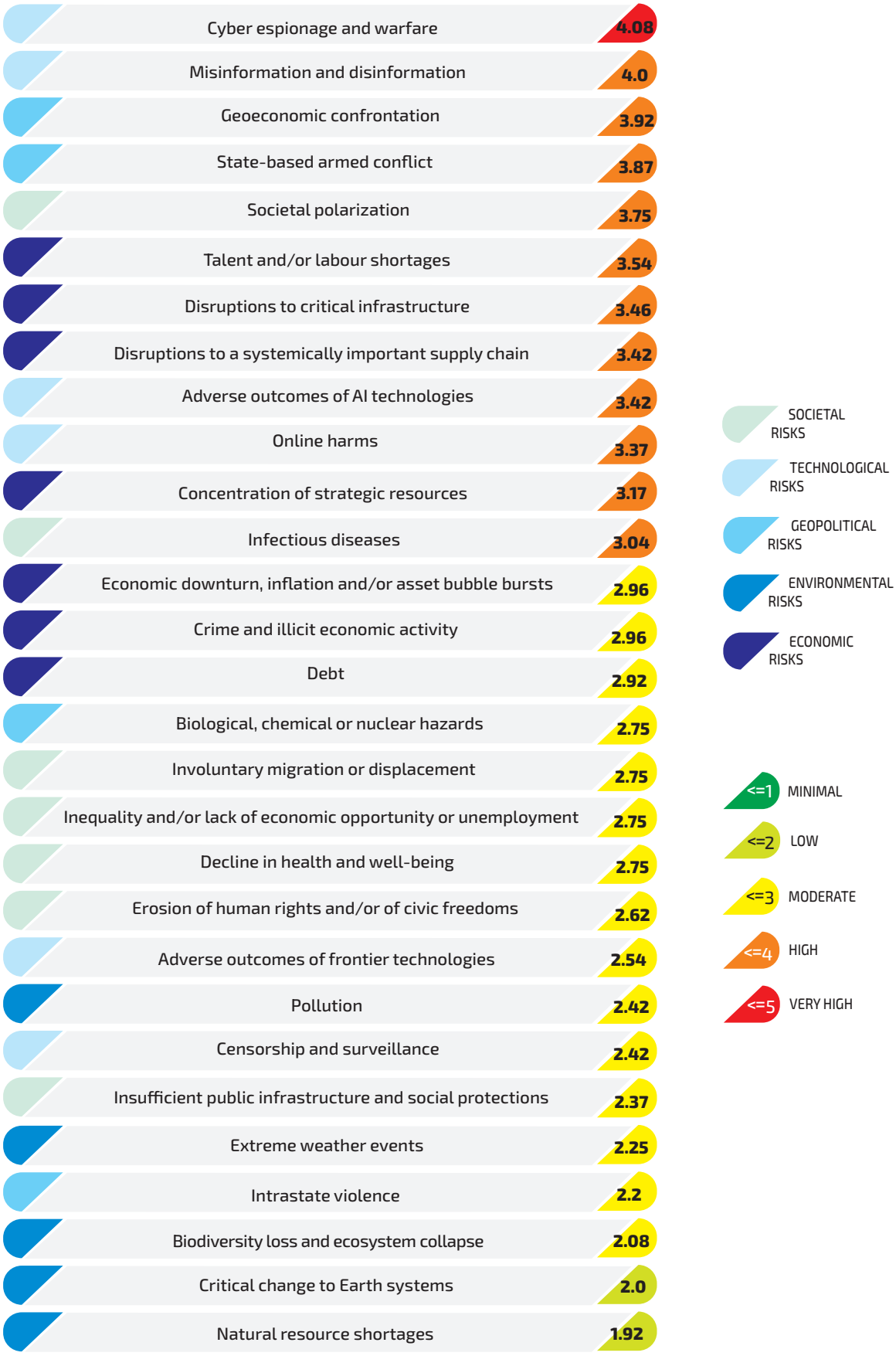

FIGURE 7. ESTONIAN EXPERTS' ASSESSMENTS OF THE RISKS WITH THE GREATEST POTENTIAL IMPACT ON ESTONIA

CYBER ESPIONAGE AND WARFARE

Estonian experts rated the potential impact of cyber espionage and warfare on Estonia as the greatest among the risks assessed (Figure 7). This risk covers (see Appendix 2) the use of cyber tools by state and non-state actors to gain control over digital environments, cause operational disruption and/or damage technological and information networks and infrastructure, including offensive and defensive cyber operations that occur during or precipitating an armed conflict, as well as cyberattacks[2] that exfiltrate classified or sensitive data or intellectual property.

Key global technological trends that are likely to affect Estonia directly and indirectly over the next five years include the rapid development of technology, notably generative artificial intelligence; increasing automation of processes; simplification of the technology user experience; growing global technological dependency, including dependence in the provision of essential services; widening shortage of cybersecurity specialists;

IMAGE: PIXABAY.COM

[2] Cyberattack is used here as an umbrella term for any malicious activity consisting of a targeted intrusion into another computer network to steal or alter data, or to damage a system. This report takes into account a diverse range of perpetrators and motives for cyberattacks.

expanding use of cloud services; accelerating simplification of executing cyberattacks; and states' rapid enhancement of military capacity through strengthening of cyber capabilities. Attention must also be paid to additional security risks that arise directly from artificial intelligence itself (Vlassov, 2025).

The principal impacts on Estonia that could result from the materialisation of these risks are:

- large-scale damage to Estonia's e-government services and a significant loss of public confidence in the functioning of the state;
- longer-term disruption to the continuity of critical infrastructure and essential services and the increased vulnerability of large population groups;
- widespread damage to defence and internal security information systems and the compromise of datasets, which would substantially degrade the state's defensive capacities and its ability to ensure internal security.

These potential impacts arise from current global developments and trends in cyber espionage and warfare, and Estonia should therefore pay attention to the explanatory factors set out below.

CYBER ESPIONAGE AND CYBERATTACKS

Artificial intelligence (AI), including generative artificial intelligence,[3] is playing an increasingly significant role in the planning of cyberattacks, enabling cyber espionage, cyberattacks and cyber warfare. It is also rapidly evolving.

The combination of the growth of big data, the rapid advancement of AI capabilities and the increasing potential for automating processes creates conditions favourable for an increase in both the number and types of cyberattacks. One trend that will affect Estonia in the coming years is the diversification of threats that follows from the ability of all states to enhance and scale up their military capabilities quickly. In this context, the increase in the capabilities of AI has produced a corresponding leap in risks related to that technology.

- AI (including generative AI) is used to conduct cyberattacks and cyber espionage, and it can automate the discovery of system or network vulnerabilities and the execution of attacks (Data Guardian Hub, 2024). Experts believe AI use may also lead to the deployment of adversarial AI designed to overwhelm system defences or to develop novel attack strategies. In addition, AI algorithms can be used to mount more sophisticated social-manipulation attacks, for example, through spear phishing or other targeted attacks that exploit information about a specific individual to trick them into revealing sensitive data. Just as AI-based methods for attacking systems can be automated, AI tools can also be employed to monitor (cyber)systems – so-called automated defence – as they increasingly are. If focused solely on threats, however, delegating tasks to AI will not necessarily make systems safer; rather, it increases dependence on technology and on its reliability across key security functions.

[3] Artificial intelligence is a set of technologies that analyse input data to emulate or replicate the logical patterns and processes involved in performing tasks. Generative AI specifically synthesises analysed inputs to produce new outputs – for example, text, images, audiovisual material or code.

- AI, especially generative AI, is increasingly used (including in the context of cyber warfare) to create fraudulent information, notably, including so-called *deepfakes* (Mahmudov, 2023). One of the most noteworthy deepfakes, for example, was a video circulated in March 2022 purporting to show Ukrainian President Zelensky urging his compatriots to surrender (Burgess, 2022). Ahead of the US presidential election in November 2024, experts judged deepfakes to be a major threat to the democratic electoral process (Taylor, 2024). Although that threat did not materialise in the US presidential election, the growing probability that many states and interest groups worldwide will use deep fakes and other forms of mis- and disinformation to influence public opinion, to undermine societal resilience and to interfere in democratic processes must be taken into account.

Companies that develop and deploy artificial intelligence, including generative AI, are concentrating on the defence sector or expanding into it.

Although the adoption of AI has grown rapidly worldwide – for example, through the widening use of OpenAI's ChatGPT, Microsoft Copilot and China's Hangzhou DeepSeek Artificial Intelligence Basic Technology Research Co., Ltd.'s DeepSeek – the sector has not yet found a way to translate the popularity of their products into sustainable corporate profitability. While AI is being used to optimise processes across various sectors, none of the companies providing those systems has so far found a product through which they can reliably recoup the costs of their development.

Nonetheless, AI developers and other large technology firms are increasingly involved in state-security processes, such as border control and intelligence collection. While building national capabilities is expensive, a private partner can help raise a state's defensive capacity at lower cost and effort.[4] Consequently, the growing pressure on states to strengthen their defence – especially in Europe – creates opportunities for defence-industry firms such as Palantir and Anduril to use classified military data to train their AI models. The state defence sector, therefore, represents a buyer with significant purchasing power.

Given the combination of AI companies' search for profitable projects with states' increasing need to improve their defence capabilities, it is likely that more AI firms will enter the defence industry. While a sharp rise in AI-based solutions in defence can be expected in the coming years, however, this will bring with it an increase in the risks associated with sharing state data with private companies, including issues of transparency and security. One immediate source of risk is the procuring of services or equipment from unfriendly states or state-owned companies. In this regard, several European countries are already taking robust steps to limit the direct use of Chinese products in defence and security, including by revising public procurement processes. Technology development chains, however, are complex and involve many parties and subcontractors. Therefore, excluding entities with Chinese participation – even from European companies – can be difficult.

A second major risk is the growing dependence of AI vendors' operations on generative AI, specifically. State–industry partnerships in developing digital solutions are not new. It has already been observed that companies developing AI solutions sometimes use generative AI in systems development in unregulated ways – even under restricted

[4] The United States armed forces have launched multiple projects that indicate a strong interest in using and integrating AI extensively in battlefield decision-making and logistics. The People's Republic of China is actively pursuing similar goals.

conditions – which can result in the system disregarding or circumventing prescribed rules (Kantrowitz, 2025). It is also common practice in systems development to reuse programming code and prompts shared on public forums, which in automated programming workflows can lead to the inadvertent integration of malicious code into a system during its development (Marcus & Hamiel, 2025).

AI-driven big-data analysis is enabling innovation in the defence industry.

AI's data-processing capabilities have already aided fields such as pharmacology and materials science, and AI is expected to enable innovation across many more domains in the coming years. These capabilities can support novel deterrence measures for defence industries, but they can equally support the development of offensive measures (O'Donnell et al., 2025). If AI can accelerate pharmaceutical development, similar capabilities could theoretically be applied to the production of chemical weapons of mass destruction. More generally, these capabilities provide states with purchasing power opportunity to rapidly scale up and diversify their military capacities.

Long-term operations allow an adversary to weaken a state and its essential services systematically and to plan physical attacks.

In the context of prolonged cyber-espionage operations and state-sponsored actors, the trends most likely to affect Estonia in the near term are those of cyberattacks conducted with state support – meaning there are sufficient financial resources available – and of attacks intended to remain undetected over as long a term as possible in order to collect information and map vulnerabilities. State actors' intelligence services (for example, Russia's GRU or the People's Liberation Army) often conduct such campaigns, but the diversification of attack vectors, AI-assisted planning and the emergence of attacks as a professional activity for organised crime (explained below) may broaden the range of actors operating on behalf of states and, therefore, make attribution more difficult. Moreover, states may deliberately maintain distance from proxy actors to preserve diplomatic relations.

Estonian public bodies and companies face constant pressure from cyberattacks. That pressure increased with Russia's full-scale aggression against Ukraine in February 2022. In 2024, the Estonian Information System Authority (RIA) recorded a record 6,515 cyber incidents that had an impact in Estonia. Worldwide, 40,287 vulnerabilities that could be exploited in cyberattacks were registered in 2024. By comparison, the global count of known vulnerabilities in 2015 was 6,487 (RIA, 2025, pp. 6, 35). Thus, both the number of cyberattacks and the volume of vulnerabilities are growing year on year, increasing the need for investment in cyber-defence by states, companies and individuals.

Recent years have seen an increase in state-sponsored cyber espionage. Moreover, cyber espionage is increasingly being conducted using the techniques of cybercrime (Deloitte, 2025; Hitachi Cyber, 2025). Advanced Persistent Threats (APTs) are becoming more sophisticated and harder to detect. Also, the exploitation of zero-day vulnerabilities and supply-chain attacks has increased. Actors seek to obtain sensitive information through long-term, targeted network infiltrations and to sabotage or disable critical infrastructure. Because of AI's utility in information processing, it has also enhanced the capacity to process and analyse large datasets quickly in cyber espionage. The digitisation of data – including state data – and the digital nature of public and essential services have therefore made such datasets key targets in the cyber-warfare context. In addition to attacking

institutions or companies, cyber espionage increasingly targets individuals for information collection.

RIA's cybersecurity yearbook (RIA, 2025) notes that China's cyber capabilities exceed those of Russia, and that China-linked groups are likely the most capable and complex anti-Western actors, distinctive for both their stealth and scale. China's cyber capability is illustrated by its extensive activity against Taiwan, which is estimated to involve some 15,000 attacks per second (see Kaljula, 2024). The yearbook also warns that products from Chinese companies subject to state control or subsidies may serve as platforms for cyberattacks.

Cyberattacks have increasingly become a component of organised crime.

Rising revenues from cybercrime and the expansion of cybercrime activities have attracted traditional organised criminal groups into the cyber arena. This trend includes the mobilisation and enforcement of groups that perpetrate cyberattacks using human trafficking to staff operations that produce and disseminate disinformation. The entry of traditional organised criminal groups into cybercrime is also changing its nature. For example, groups accustomed to causing physical harm may be less inhibited about attacking critical infrastructure, or they may accept clients for ideological reasons.

The rapid integration of new AI-based technologies and a growing shortage of cybersecurity specialists.

In the near term, the trends most likely to affect Estonia are insufficient consideration of risks when integrating AI and a shortage of skilled personnel needed to implement additional security measures.

Tools based on AI, including generative AI, have been rapidly integrated into many workflows because of their ease of use, and many regard mass-market generative AI (for example, ChatGPT, Copilot, DeepSeek) as a major aid for optimising the efficiency of everyday tasks. Despite the rapid adoption of AI, however, the *World Economic Forum's Global Cybersecurity Outlook 2025* reports that only around one third of companies surveyed had security protocols in place to assess the safe integration of AI systems before deploying them. For certain tools, such as services provided by Chinese firms, practical and state concerns about security risks have been raised in Estonia and other countries. Nonetheless, the use of AI tools remains largely unregulated. Regulation may appear less necessary when an AI-based service is supplied by a software vendor whose products are already in use in a state body, agency or company. However, excessive trust in the deployment of AI systems can lead to undetected and novel risks emerging. In particular, cloud technologies – on which many AI tools depend – are widely seen as a significant future vulnerability.

Training and labour-market supply lag behind rapid technological development. Consequently, both Europe and Estonia face an increasing shortage of cybersecurity specialists (European Commission, 2024a). The 2024 Eurobarometer survey found that, in Estonia, over three quarters of employees working in cybersecurity had moved into that role from other duties rather than being recruited specifically for a cybersecurity post (the European average is 57%). Estonia also lags behind the European average on indicators such as transition into cybersecurity roles and the proportion of workers in their first specialised cybersecurity job (European Commission, 2024b). In short, cybersecurity roles in Estonia are often performed by people without formal qualifications for the task. In an

increasingly complex cybersecurity landscape, this is an alarming trend for a digitally enhanced state.

CYBER WARFARE

Degradation of national communications infrastructure to enable an invasion or an information operation.

Although experts' expectations of large-scale communications outages in Ukraine at the outset of the 2022 invasion did not materialise, Russia's past tactics include similar actions that could have direct implications for Estonia. For example, the degradation of communications infrastructure played a key role in the annexation of Crimea that enabled Russia simultaneously to seize local control and to flood the international information space with misinformation (Pickle, 2024). Because this tactic remains in Russia's arsenal, the resilience of communications infrastructure running through the Baltic Sea and the activities of shadow fleets friendly to Russia in the northern Baltic region must be monitored and countered with vigilance (Loik, 2024; Muuga et al., 2025).

It is important to stress that Russian intelligence services seek access to information of national importance. Information protection, therefore, requires systematically assessed strong cryptographic solutions (Välisluureamet, 2025, p. 9). The Internal Security Service also warns that units conducting cyber-intelligence operations actively seek access to Estonian state and private networks and, at the same time, trends point to the growing exploitation of compromised devices and use of botnets for intermediary attacks (Kaitsepolitseiamet, 2025, p. 38).

Russia employed a range of information operations and cyber-enabled information operations as an integral part of its hybrid hostility against Ukraine in the escalation phase preceding its conventional attack, its aim being to shape the strategic and operational environment in its favour. Various "hack-and-leak" cyber operations were conducted. Particularly damaging were the use of destructive malware and attacks on essential state services, databases and elements of critical infrastructure (Savimaa & Loik, 2023, p. 38). Estonia must be prepared to counter similar cyber operations both within state institutions and in private companies of systemic importance. A significant recent risk is the vulnerability of submarine links that form critical infrastructure (Muuga et al., 2025), including sabotage threats to the security of information-communications and energy systems.

Cyber–physical attacks to degrade national (vital) infrastructure and trigger a civilian crisis.

Although energy dependence in a digitally enhanced Estonia is not a new threat, the continual rise in dependence on electricity for technology-enabled services makes the risk to energy infrastructure increasingly consequential: disruption could paralyse the functioning of a digitally enhanced state. Other vital infrastructures – water and sewage networks, transport and so on – also depend on the availability of electricity. As the capabilities of the technologies to conduct cyberattacks advance, so does the feasibility of strikes against infrastructure. Infrastructure failures caused by such attacks can be

exploited to facilitate an invasion or to secure advantage in a (cyber)war by changing the balance of power.[5]

Rather than decisive offensive strikes, cyber operations have mainly supported conventional warfare by enhancing reconnaissance and intelligence.

Continued hostilities in Ukraine have provided an opportunity to analyse the tactics and domains of (cyber)warfare more closely based on the example of Russia's conduct. In this regard, it appears that cyber warfare is not primarily an offensive exercise in the kinetic sense, but that its principal sphere is the collection of intelligence. Some experts consider this the "best" use of the cyber domain (Pickle, 2024). Given the developments in cyber espionage described above, the cybersecurity of state services and datasets will become even more important in future. Intelligence obtained through espionage can lead to the leaking of information that directly threatens a state's operational and defensive capacities and can be used in a targeted manner to weaken those capacities.

Large technology companies such as Starlink, Google and Amazon play an increasing role in (cyber)wars.

In crises and situations where national infrastructure is disrupted, large corporations can provide essential aid to the state and the functioning of its infrastructure. Partnerships with global technology firms can, therefore, be indispensable for providing vital services and for supporting the armed forces, the economy and state functions. It is important to note that services provided by private companies can be accessible to all actors whose purchasing power and ideology fit the supplier; hence, establishing and maintaining partnerships requires careful assessment and mitigation of the risks these relationships create with respect to access to resources and infrastructure. In practice, a state can become dependent on a service provider's rules and pricing, as well as on the provider's willingness to continue the service. These are so-called key terrains in the cyber domain. National partnerships and agreements with international IT companies are therefore becoming ever more important, and Estonia should carefully assess other states' behaviour and secure its own position.

Technological development is making the nature of cyber warfare increasingly complex and harder to detect, and the ease of conducting operations is raising its likelihood. Estonia therefore needs to strengthen its capacity for critical analytical assessment.

The use of cyber and physical measures in warfare has so far not followed analysts' earlier predictions (see Pickle, 2024), whereby activity in one domain would directly empower the other. It is, therefore, important to analyse alternative modes of cyber war – including cyber activity that enables action in the physical domain and cyber activity used to prepare a physical attack. Further analysis of cyber warfare is of critical importance to Estonia because neighbouring Russia has repeatedly demonstrated the ability to threaten the stable functioning of (democratic) society through cyberattacks. When analysing the motivations for using cyber measures, two principal trends should be borne in mind:

---

[5] According to the World Economic Forum, only 50% of surveyed experts were "confident" or "very confident" that their organisation or state is well prepared to prevent and manage major cyber incidents targeting critical infrastructure (World Economic Forum 2025, p. 6).

- The war in Ukraine shows that cyber operations are used to influence and control the attitudes of target groups in the information environment and to achieve and maintain strategic initiative.
- Cyber operations without a coordinated physical attack have not proved sufficient to gain physical control of territory. Coordinating cyber and physical attacks, however, has proven very complex in the Ukrainian war.

In cyber warfare, hostilities do not occur solely between two states; cyberattacks also draw in additional actors.

Whereas conventional warfare centres on confrontations between states' armed forces, cyber warfare is likely to involve a broader array of participants, including supporting and contracted forces. The trend of increasing a state's military capacity by incorporating other parties may affect Estonia in the coming years. A state's capability to wage (cyber) war should, therefore, not be assessed only by the size of its official units but must also take into account potential collaborators. This, in turn, means that cyberattacks against a state and its infrastructure should be assessed accordingly: they may not be discrete, unconnected strikes by separate actors, but parts of a systemic, coordinated campaign directed at the target state and carried out by actors supported and recruited by the aggressor. (Pickle, 2024)

MISINFORMATION AND DISINFORMATION

Estonian experts rated the spread of misinformation and disinformation as the second most consequential risk for Estonia. This category refers to the continuous dissemination of manipulative information across media networks by state and non-state actors, intended to skew public opinion significantly by undermining trust in facts and authority, including through false information and fabricated content.

Under the Penal Code (*Karistusseadustik* as of 25 July 2025), Estonia criminalises calls for war or other uses of armed force that contravene generally recognised principles of international law (Section 92, "Propaganda for war"). Incitement of hatred is also criminalised (Section 151) – that is, acts that publicly call for hatred, violence or discrimination on grounds of nationality, race, skin colour, sex, language, origin, religion, sexual orientation, political beliefs, property or social status when such conduct endangers a person's

IMAGE: MICROSOFT COPILOT, 2025

life, health or property. Supporting or justifying an international crime is criminal (Section 151[1]) – for example, the public display of a symbol associated with aggression, genocide, crimes against humanity or war crimes in a way that supports or legitimises those acts – and public calls to commit a crime against the Republic of Estonia are punishable by law (Section 236). Hostile influence operations that fall below the criminal threshold, including those originating outside the jurisdictions of Estonia and the European Union, increasingly demand attention and active countermeasures, such as public exposure of information-operation content and sources, the development and enforcement of media sanctions, and other responses.

The principal negative impacts of hostile influence activity on Estonia are likely to be:

- reduced public trust in the legitimacy and effectiveness of democratic institutions;
- deepened societal polarisation, creating fertile ground for the radicalisation of particular groups;
- diminished credibility and effectiveness of Estonia's foreign and security policy on the international stage.

In discussions of hybrid threats, increasing attention has been paid to the vulnerabilities of democratic political systems and decision-making processes to hostile manipulation attempts, particularly in the information environment (Savimaa et al., 2024, p. 8). The current Russian regime has made purposeful influence over the information space a central element of its strategic offensive toolkit. This tool is used actively both domestically and internationally, including to interfere in democratic elections (see Duffy and Harbath, 2024; Zygar, 2024). Given the likely continuation of the present political system in Russia, it would be naïve to expect its aggressive sphere-of-influence strategy towards neighbouring states and their allies to change (Loik, 2022). On the contrary, Kremlin disinformation methods are becoming ever more diversified. This development demands greater strategic attention, strengthened resilience and clear policy responses from Western states and democratic institutions if the credibility and resilience of democratic decision-making are to be preserved under intense information warfare. It is also important to deepen EU–NATO cooperation on hybrid threats (Zandee et al., 2022).

Innovations in the application of artificial intelligence create new strategic advantages, dilemmas and security problems for the planning and conduct of hybrid operations in the information environment. The Internal Security Service (Kaitsepolitseiamet, 2025, p. 43) forecasts an increasing role for AI in manipulative influence operations aimed at disrupting elections and other democratic processes. Such information operations, moreover, are becoming more complex and more extensive. **The use of AI in information operations introduces the risk of massive, fast and precisely designed hostile influence campaigns and cyber-enabled information operations.** At the same time, hostile actors' intelligence and analysis capabilities are increasing, which, in turn, enhances their ability to identify vulnerabilities in complex systems and to trigger escalating cascade effects.

Recent reports and yearbooks of Estonia's security agencies (the Internal Security Service and the Foreign Intelligence Service) have consistently drawn attention to security threats originating in China. The Internal Security Service's yearbooks have highlighted activities by the PRC embassy and representatives of Chinese communities in Estonia as factors intended to influence public opinion and to propagate attitudes favourable to

China. The 2023–24 yearbook also notes that, compared with Russia, Chinese intelligence activity is broader and more intensive (Kaitsepolitseiamet, 2024, p. 21), encompassing all areas from military, technical and scientific espionage to cyber espionage and attacks to instruments of soft power such as cultural cooperation. Active and passive influence operations and the recruitment of agents of influence from local populations are central to this activity.

China has built a global intelligence network that operates through mechanisms such as the United Front directed by the Communist Party of China (CPC's) international relations apparatus, which organises Chinese nationals living abroad. According to Australian analyst Alex Joske, this network focuses on recruiting "people in positions of influence […] who claim to represent major segments of society – community leaders, business magnates, religious figures" (Joske, 2022, p. 31; Läänemets, 2024, pp. 21–22). In Estonia, China has engaged in similar influence activities, as Estonian China expert Frank Jüris points out: "although China's success has been partial, its influence activities have reached the highest levels of Estonian politics" (Jüris, 2023, p. 3).

In 2024, a high-profile visit by members of the Estonian parliament's Estonia–China parliamentary group – partly financed by Chinese sources – and the ensuing public debate, in which the PRC embassy also intervened, attracted considerable attention (Madsen, 2024). As public awareness and critical scrutiny of Chinese influence activity have grown in Estonia, the embassy has shifted some of its activities towards Estonia's local governments. This includes organising meetings and cultural events for local governments, as well as setting up educational institutions and businesses that might serve propaganda purposes (Lomp, 2025). The Internal Security Service takes the view that, because China is not a friendly state and tends towards cooperation with a state hostile to Estonia – Russia – all of the PRC's activities in Estonia should be viewed through a security lens, taking into account that "China itself examines all activities from the standpoint of security and the CPC's maintenance of power" (Kaitsepolitseiamet, 2025, p. 33).

INTERSTATE ARMED CONFLICTS

Estonian experts ranked the risk of interstate armed conflict as the third most consequential threat to Estonia's security. This category encompasses the use of force by two or more states and/or between states and non-state actors, often for ideological, political or religious purposes, and manifesting as war and/or organised, sustained violence – including active hostilities, insurgencies, civil wars, terrorism, genocide and assassinations.

The most significant impacts on Estonia if such risks materialise could include:

- rapid escalation of political polarisation and conflict;
- an increase in hostile influence activity;
- a heightened threat to constitutional order and territorial integrity.

The threats associated with interstate or state–non-state armed conflicts are diverse. In Estonia's security context, the Russian war of aggression in Ukraine and armed conflicts in the Middle East remain central threats, both of which have contributed to polarisation

IMAGE: STOCKCAKE.COM

and radicalisation within Estonia. The effect of an interstate armed conflict, or of other forms of organised violence, on Estonia's internal security depends on the size of the communities connected to the conflict and on the influence of external actors. The most severe scenario for Estonia would be the occurrence of such conflicts in its immediate neighbourhood.

Contemporary armed conflicts are often part of a broader hybrid contest in which, alongside direct kinetic confrontation between parties, proxy warfare takes place on third-country territory, employing, among other means, locally based criminal actors or extremists recruited online. To pursue their objectives in third countries, the intelligence services of Iran, Russia and China have increasingly relied on criminal networks to conduct both physical and cyberattacks and to run disinformation campaigns (DOJ, 2023; Kaitsepolitseiamet, 2024, 2025; Europol SOCTA, 2025; ISCP, 2025; Jones, 2025; PST, 2025).

Threat assessments for Estonia should monitor developments in the Middle East and Europe.

The 2015–16 migration crisis arising from the Arab Spring and the Syrian civil war demonstrated that even relatively short-lived waves of violence in the Middle East or North Africa can have long-term effects on European Union Member States. Border security in particular comes under heavy strain, and the capacity to manage large irregular migration flows is tested. Such crises can also lead to travel to conflict zones to join fighting with terrorist groups, financial support for those groups, and the dissemination of terrorist propaganda. Lone-actor terrorist attacks also remain a source of risk. It is highly likely that Russia will seek to exploit situations of armed conflict to foment division within Western societies and within Estonian society.

Conflicts involving state actors increase the terrorism threat in Europe.

Interstate armed conflicts often shape terrorism trends: they can drive the spread of extremist ideologies, encourage new alliances and affect attack tactics. Military conflicts can act as a trigger for radicalisation, create fertile ground for extremist views to spread and facilitate the movement of foreign fighters into conflict zones. They can also generate societal polarisation in countries that are geographically distant from the fighting and not directly affected by hostilities.

Interstate conflicts are often accompanied by the accelerated adoption and diffusion of new military technologies. This dynamic raises significant security concerns in the context of drone warfare, especially as knowledge and capabilities become available to non-state actors. Terrorist organisations and international criminal cartels have shown growing interest in acquiring drone-warfare expertise for the battlefield (Altman, 2025; Höller, 2025). The potential use of commercial drones by violent extremists, including lone actors, is an increasing terrorism threat (Hambling, 2025; Rassler & Veilleux-Lepage, 2025).

Counter-terrorism measures in Western countries and regional cooperation remain crucial for preventing terrorist attacks and their instigation. These efforts have reduced the capacity of international terrorist organisations to mount cross-border operations. Cross-border terrorist propaganda and propaganda that justifies terrorism will remain a persistent problem in the online environment. New technological developments amplify this challenge and increase the vulnerability of ever younger cohorts to such propaganda.

The war Russia is waging against Ukraine has been accompanied by a broader Russian and Chinese anti-Western hybrid campaign.

Beyond disinformation and influence activity, operations carried out in Europe as subcontracted tasks by Russian intelligence services or criminal networks have included attacks on critics of Russia and political opponents, vandalism, arson and other acts of sabotage, including against critical infrastructure (Edwards & Seidenstein, 2025). China has also played a role in this campaign. As an avowed strategic partner of Russia, China has amplified Moscow's agenda both domestically and internationally. China's economic and political support for Russia, as well as its military cooperation with Moscow, enable Russia to persist in its war against Ukraine – representing a direct, tangible security risk to Estonia and to Europe as a whole. China pursues its partnership with Russia and its earlier posture of ostensible neutrality in the Russia–Ukraine war chiefly to advance its own global influence (see Läänemets, 2023). China's foreign minister has publicly stated that China cannot allow Russia to be defeated in the war in Ukraine (Walsh, 2025).

If China were to attack Taiwan in the near term and trigger a new war in the Indo-Pacific that draws in the United States and its allies – an outcome many experts still judge unlikely despite rising tensions and hostile rhetoric from Beijing (see Läänemets, 2022; Adlakha, 2023; Roy, 2024) – the consequences would be unpredictable worldwide. Such a conflict could escalate across the Indo-Pacific and would probably increase pressure from Russia on Europe. Estonia's security would also be affected, primarily through disruptions to supply chains that could produce shortages of certain consumer goods and interruptions to the delivery of equipment and technologies to strategically important facilities, for example, solar and wind energy parks.

Broad terrorism trends indicate that violent Islamist extremism will remain the principal global terrorism threat.

In the coming years, terrorism will continue to be shaped by political and military developments in the Middle East. The near future will reveal what form a new Islamist regime in Syria will take and what regional position it will assume, as well as what role Turkey will play in events there. Based on current trends, violent jihadism – violent Islamism/Islamist extremism – is likely to represent the greatest terrorism threat in Europe and globally (Europol TESAT, 2025; GTI, 2025). The terrorism threat in Europe could increase if a terrorist group establishes control over territory and proclaims a proto-state, thereby becoming a magnet for recruits from Europe (cf. ISIS in 2014–2019) (Europol TESAT, 2025). It can be expected that attackers in Western countries will increasingly be lone actors radicalised online, inspired by terrorist ideology and propaganda materials but without formal or direct ties to any organised group (Europol TESAT, 2024).

GEOECONOMIC CONFRONTATION

The risk ranked fourth by Estonian experts in terms of potential impact was geoeconomic confrontation. This category refers to the use of economic instruments by global or regional powers to reshape interstate economic relations by restricting the movement and diffusion of goods, knowledge, services or technologies in order to enhance self-reliance, constrain geopolitical competitors and/or strengthen spheres of influence – for example, through currency measures, investment screening, sanctions, state aid and subsidies, and export controls.

The most significant impacts on Estonia if such risks materialise could include:

- negative effects on the Estonian economy resulting from unpredictable and volatile United States foreign economic policy;
- disruptions to supply chains important to Estonia;
- direct and indirect economic effects in Estonia arising from sanctions imposed by the European Union and the United States against Russia and Belarus.

IMAGE: MICROSOFT COPILOT, 2025

Geoeconomic confrontation is deepening and reshaping the global balance of power.

In the oming years, the levers that will determine the balance of global power are likely to be control over the foundations of the world economy: data centres, chip factories, cobalt deposits, transport corridors and, above all, the rules that govern their use. Washington – together with the EU – and Beijing – together with an expanding BRICS bloc – are already ensuring the separation of distinct technology and resource spheres. The dominant coalition will be whichever is best able to exploit supply chains, standards regimes and market positions. Moreover, in a world where artificial intelligence is becoming the principal driver of economic development, military power will also matter for defending an economy that is increasingly value-based and geographically distributed.

The United States routinely sends ambiguous economic-policy signals.

President Donald Trump frames US tariffs as punitive measures, but the coherence of his initiatives is questionable. In practice, such actions have already sown confusion in the global economy, prompting all countries – including former allies – to seek the best arrangements for them individually while simultaneously attempting to reduce their economic dependence on the United States (Manak et al., 2025; Puri, 2025). The consequences of this may include, among other things, a diminished role for the US dollar as the world's base currency and increased volatility in oil prices.

The direct effect on Estonia of protectionist tariffs imposed at President Trump's initiative would stem chiefly from our reliance on international trade and on the economic health of trading partners. Although Estonia's direct commercial ties with the United States – excluding the defence industry – are relatively modest, global market instability would nevertheless have a negative effect on the EU economy and, therefore, on Estonia. EU countermeasures would mitigate some of these effects, the scale and scope of which will depend on the concrete steps taken by the United States. It is also important to recognise the EU's general dependence on imports and global supply chains and to monitor the potential growth of Chinese influence in Europe.

China is increasingly using economic and trade dependence as a tool of political influence.

The principal geoeconomic security risk stemming from China is the extent to which China can make other states dependent on its strategic raw materials, technologies, investments and consumer goods. China's import volumes may come to depend on tariff arrangements between China and the United States. If China is unable because of high tariffs to export to the United States at former volumes, it will seek new markets for its goods – primarily in Asia but likely in Europe as well, including Estonia. In that situation, Estonia might prefer an increased inflow of cheaper Chinese goods, while higher-priced Western products would be less competitive. This trend could be driven, in particular, by Estonia's sharply increasing cost of living, falling purchasing power and widening social and economic cleavages, themselves a consequence of higher tax burdens and the need to divert resources from long-term economic priorities into rapidly accelerating defence readiness.

Beyond a certain threshold, such trade dependence can translate into political dependence: populist politicians may invoke improved material conditions to pursue a significantly more China-friendly policy, as has occurred in several Central and South-Eastern European countries (for example Hungary and Serbia), whose governments have

remained consistently pro-China and in which China has made large investments (Rohac, 2024, pp. 3–4). These countries stand out within Central and Eastern Europe for their friendliness to China, which is clearly correlated with their pro-Russian policies.

Estonia has limited manoeuvring space here because it is heavily exposed to the trade policies of great powers. If the United States and China reach a tariff agreement that does not materially disrupt global supply chains, which is a plausible scenario, Estonia's situation in terms of the supply of export goods at acceptable prices may not change significantly.

EU and US sanctions on Russia require more effective enforcement.

On 18 July 2025, the European Union adopted its 18th package of sanctions against Russia (a 19th is underway), a central measure of which lowers the Russian oil price cap from 60 US dollars to 47.60 US dollars per barrel. The cap will be reviewed every six months to ensure it remains 15% below the average market price (Eesti Vabariigi Välisministeerium, 2025). The EU has taken a principled decision to eliminate reliance on energy sources from Russia (oil, gas, uranium) by 2027.

For Estonia, the 2027 change will have only a limited direct effect, since Estonia's direct economic ties with Russia had already declined year on year before the current confrontation intensified. Russian oil and gas have not been imported directly into the Estonian market for years (for example, Lukoil left the local market in 2003), but given the structure of EU energy markets, it is plausible that some refined products on the market may originally derive from Russian crude (Suzan & Bounfour, 2023). At the EU level, the need to strengthen sanctions enforcement has been recognised, which requires additional resources from competent national authorities. On 24 April 2024, the European Parliament and the Council adopted Directive (EU) 2024/1226 on penalties for the violation of Union restrictive measures, which obliges Member States to criminalise the activities defined in the directive under national law. Harmonisation is principally needed for criminal penalties relating to failure to freeze assets, breaches of travel bans and arms embargoes, the provision of prohibited or restricted economic and financial services, and the submission of false information concerning sanctioned assets (Bonifassi & Bastien, 2025).

In summary, the world has entered a phase of geoeconomic ambiguity and volatility. The growing economic friction between Europe and the United States is hopefully temporary and reversible, and in the longer term this may lead to a renewal and strengthening of allied relations. Estonia has long chosen to belong to the West and there is no reason to reconsider that choice. At the same time, current trends should be treated not only as problems but as challenges and opportunities to better integrate the economies of Estonia and the West, especially EU Member States, thereby ensuring stable socio-economic development in Estonia. Estonia's relative smallness and resulting flexibility allow it to adapt to changing markets and production patterns quickly and efficiently.

SOCIETAL POLARISATION

Estonian experts rated threats arising from societal polarisation as the fifth most significant risk to Estonia. This category covers ideological and cultural divisions within and between communities that undermine social stability, an inability to make decisions, economic disruption and growing political polarisation.

The most significant impacts on Estonia if such risks were to be realised include:

- paralysis of the decision-making required to safeguard the state's economic stability;
- intensified division between communities, in turn, generating rising social instability;
- increased uncertainty and negative trends in the investment climate and consumer behaviour.

Global polarisation, growing populism and declining engagement are all structural challenges for Western democracies in the first quarter of the 21st century (Borbáth et al., 2023; Serani, 2025). Polarisation occurs when there is conflict of social and political values. In the contemporary period, this has been amplified by social media (Yarchi et al.,

IMAGE: MICROSOFT COPILOT, 2025

2020; Kubin and von Sikorski, 2021) and is likely to be further exacerbated by the use of artificial intelligence to manipulate public opinion. Over the past decade, Western societies have experienced a sequence of crises that have been accompanied by growing societal and political polarisation. Migration crises, climate anxiety, the pandemic, Russia's war of aggression in Ukraine, the Hamas–Israel confrontation in Gaza and battles over identity rights are among the broad set of polarising issues at political, social and cultural levels.

There is reason to expect that, in the coming years, attitudes, values and positions will become more radicalised and polarised across multiple domains.

Societal and political polarisation in Western democracies can be expected to increase as a consequence of both global and local crises. Rapid technological, geopolitical and socio-cultural change has amplified conflicts of values. At the same time, hostile state and external non-state actors seek to magnify existing divisions within societies, if necessary, by supporting opposing views and extremist groups.

In hybrid warfare, efforts to undermine Western unity combine cyber, criminal and cognitive tactics. AI-generated disinformation is used to undermine the credibility of democratic institutions and the media. Internet echo chambers and social media algorithms undermine social cohesion and create or intensify polarisation. Processes of alienation from power and population decline in peripheral regions are exploited by actors with various extreme ideologies opposed to liberal democracy. Populism is becoming a mainstream phenomenon across the political spectrum. In the West, debates over migration and integration continue to be a contributing factor to polarisation.

The targeted use of artificial intelligence by hostile actors is predicted to further increase societal polarisation by 2030.

Mainstream adoption of AI has brought a paradigm shift to how misinformation is disseminated and operations intended to shape narratives are conducted. Deepfakes, synthetic media and algorithmically hyper-personalised propaganda blur the line between authentic and manipulated information and intensify existing polarisation. In information warfare, even otherwise effective counter-narratives may be drowned out by the cacophony of the vast body of AI-generated material. By undermining the credibility of democratic institutions and the media, this dynamic can threaten the foundational pillars of public discourse.

Conflict narratives (for example, global jihad, Western oppression, Russian resistance) are now consumed at high speed on TikTok, YouTube Shorts, Discord and Telegram (Shin & Jitkajornwanich, 2024). Platforms amplify emotionally charged material, which is often poorly moderated. Internet environments remain a major channel for radicalisation into extremist ideologies. A growing problem is the radicalisation of early adolescents into violent ideologies. In 2024, 16% of those detained in Europe on terrorism charges were aged 12–17 (Europol TESAT, 2025).

The radicalisation of ever younger cohorts into extremist worldviews will remain a problem in the years ahead. Young people are vulnerable to extremist content because they increasingly encounter unregulated online subcultures that expose them to extremist material and conspiracy theories (OECD, 2023). Mental-health problems, isolation and a lack of belonging among youth deepen this vulnerability and increase their receptivity to such content, while manufactured distrust and anger stoked by fake news, memes and

influencer-led propaganda are exploited to manipulate them. Right-wing memes, jihadist videos and anarcho-nihilist subcultures can radicalise individuals through gaming and meme cultures at a point before they come into contact with institutional safeguards.

As this decade has shown, societal polarisation can take hold across many spheres of life, wherever value conflicts provide fertile ground. Groups with a range of extremist ideologies and worldviews – whether political, religious or cultural – exploit sensitive issues to erode trust in state institutions and the democratic decision-making process. AI has made the creation and dissemination of disinformation faster, cheaper and harder to detect than before, providing a powerful tool with which to undermine institutional narratives and silo people in competing realities.

Without effective prevention and countermeasures, hostile external actors – state and non-state alike – as well as local content creators and networks will increasingly be able to exploit emerging technologies and asymmetrical tactics to deliberately deepen social divisions. Moreover, a serious challenge to prevention and response is posed by technological developments, including *malicious AI swarms* (Schroeder et al., 2025), that require the development and deployment of specific software security solutions.

COMBINED IMPACT OF THE REALISATION OF POTENTIAL RISKS

Estonian experts (this report, p. 14) assessed the threats most likely to affect Estonia in the coming years as cyber espionage and warfare, misinformation and disinformation, interstate armed conflict, geoeconomic confrontation and societal polarisation. The following considers the threats most likely to affect Estonia through the lens of four internal-security domains: border security; the functioning of critical infrastructure and essential services; civil protection and community crisis preparedness; and societal security (Figure 8).

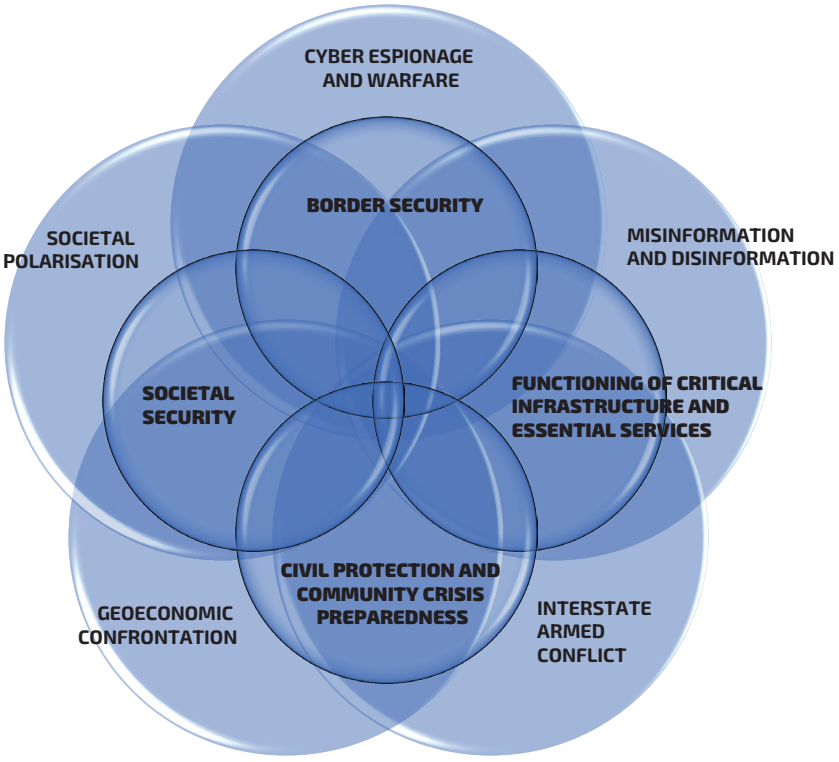

FIGURE 8. ADDRESSING THE RISKS MOST LIKELY TO AFFECT ESTONIA ACROSS FOUR OPERATIONAL DOMAINS

Researchers also analysed possible cascade effects and the combined impact of risks materialising in these four domains simultaneously. The review also takes into account the World Economic Forum's assessment of the highest-impact risks presented above (this report, p. 7). Though some items on this list (for example, extreme weather events) may not have been judged by Estonian experts to represent the most immediate or direct threats to Estonia, they nevertheless have the potential to affect Estonia's internal security and safety indirectly.

The simultaneous occurrence of multiple global risks and their mutual synergy can produce cascade effects that escalate crises into broader and harder-to-manage societal problems. Where several crises unfold at once, existing measures that might have sufficed for responses to single-event responses may prove inadequate. Normal reserve stockpiles and plans can be insufficient if multiple essential services are disrupted concurrently. The potential for such escalation through cascade effects increases community vulnerability, with economic instability, deepening social cleavages and the erosion of public trust in state institutions often following. It is, therefore, essential that internal security agencies and other state-sector institutions have the preparation plans, strategies and risk-management processes required to anticipate and be fully ready for situations that demand greater resources or have unexpected dynamics. It is equally important that legislation governing internal security is kept up to date and aligned with rapidly evolving technology and changing conditions, including economic conditions.

BORDER SECURITY

Cyber espionage and potential cyber warfare conducted by Russia, China, and other states or interest groups may involve cyberattacks targeting systems used in border policing, such as surveillance networks, biometric databases and migration-control platforms. Such attacks can bring border-control processes to a halt, cause false alerts in surveillance systems, and/or allow the manipulation of transmitted data, thereby degrading situational awareness. For example, cyber manipulation of automated border-control points (for instance, e-gate systems) may lead to longer queues, undermine confidence in both technical systems and the Police and Border Guard Board (PBGB), and increase the risk of unlawful crossings along the green border. Cyber espionage makes it possible to obtain sensitive information on border management and tactical border-defence arrangements (such as sensor placement, patrol organisation and responses to alerts), which can later be used to plan smuggling, sabotage and physical attacks. An additional risk arises from technology solutions manufactured in China, such as surveillance-service platforms that, without proper administration, can become covert channels for unauthorised access to systems and data. If appropriate security measures are not implemented, cyberattacks can also directly incapacitate border-policing technologies (for example, drones, surveillance systems and databases).

Misinformation, disinformation and Russian strategic influence operations can promote falsehoods – disseminated via the media and through official or other direct channels in third countries, EU Member States and Estonia – about "open border" policies, refugee rights and conditions for crossing borders. Such misinformation may result in irregular migration flows that can be exploited as hybrid-pressure measures, as occurred in 2021 on the Belarus–EU border. Russian influence operations may spread narratives that erode public trust in the PBGB, including by portraying border guards as inhumane or biased towards refugees. Disinformation can escalate tensions in border areas by, for example, cultivating the idea among local populations that they will be harassed and

dispossessed if new border zones are established. Misinformation can also be used to polarise border communities, which, in turn, can reduce locals' willingness to cooperate with border authorities, thereby weakening their early threat detection capabilities. In sum, misinformation and disinformation are effective means to undermine public trust in border and migration policy.

Russia's aggression in Ukraine has generated refugee flows that include applicants using Russian-established crossing points. This increases the burden on Estonia's border-control system and requires both flexibility in migration-management mechanisms and continuous monitoring to detect potential security threats. Though not yet widely recorded, it is possible that terrorist groups or foreign fighters could infiltrate mass immigration flows from third countries, which would place further pressure on biometric identification and risk-profiling systems. While assessments of Russia's military capability vary, an escalation of the conflict in Ukraine – whether favourable or unfavourable to Russia – could prompt Russia to carry out diversionary acts at the borders with the Baltic states, for example, to test NATO's response capabilities near the frontier or to generate unease and fear within Baltic societies.

Russia's war in Ukraine, NATO states' support for Ukraine's independence and territorial integrity, and Russian statements calling for a reduced NATO presence near Russia's borders constitute a potential direct threat to Estonia's border security and imply possible hostile actions by Russia at EU borders, including Estonia's. One example of explicitly hostile behaviour would be the unilateral removal of navigation buoys placed in the Narva river as a result of previous bilateral agreements. Russia has also carried out extensive GPS jamming in the St Petersburg and Pskov regions, reportedly to interfere with Ukrainian drones, with no apparent regard for the international impact on civil aviation safety in other states. Targeted drone incidents may also increase in scope and severity, which would require the rapid development and deployment of counter-drone measures.

The fourth risk – geoeconomic confrontation between Russia and the EU and its Member States – also affects border security. For example, widened sanctions regimes may act as a stimulus for smuggling networks and increase the risk of corruption in border crossing operations. Illicit trade becomes more attractive under economic pressure. Accordingly, if economic vulnerability rises among border communities in south-east Estonia and Ida-Viru county, this may boost support for the shadow economy and lead to breaches of laws regulating border crossings. Direct Russian activity, carried out under the perception that the EU and its Member States are geoeconomic and geopolitical adversaries, can also impede both the operation of crossing points and control of cross-border contraband on the Russian side. Additionally, as with the organised irregular migration crisis at the Belarus–EU border in 2021 and the intensification of irregular crossings on the Russia–Estonia and Russia–Finland borders, the volume of irregular migration along the Russia–Estonia border may also increase.

The fifth risk – societal polarisation – can affect border security by fragmenting social consensus on migration policy and border control, for example, over the reception of asylum seekers or the intensity of border protection. If part of the population views border policy as ideologically motivated (whether it is seen as too lenient or too strict), public debate may become more intense. Fragmentation of the information environment can prevent a shared public understanding of real border threats, which, in turn, can undermine cooperation in a crisis. External actors (for example, Russia or China) may drive radicalisation to exploit societal divisions and mobilise border-area populations for anti-EU or anti-NATO information campaigns. For instance, strongly pro-Russia groups in bor-

der regions, coordinated by Russian organisations, could organise small acts of sabotage or demonstrations intended to disrupt operations and security at border control points.

Global threats may affect Estonia's border security. Extreme weather, interstate armed conflicts in regions outside Europe and terrorism can all substantially increase migration pressure, especially from the Middle East and Africa. This may create a logistical and operational overload for Estonia's border-management system.

Recommendations for managing internal security risks over the next five years:

- Strengthen the digital and physical resilience of border and migration systems and ensure that they are continually updated.
- Continually update crisis-management plans and adjust them to cover the possible combined effects of migration pressure and information operations.
- Assess the dependence on and vulnerability of border-security systems to third-country technology providers and implement technical and organisational measures based on that risk analysis.
- Rapidly develop and deploy counter-drone capabilities.

CRITICAL INFRASTRUCTURE AND ESSENTIAL SERVICES

Systemic cyber espionage and targeted cyberattacks can simultaneously incapacitate multiple essential services and infrastructures, producing cascade effects throughout service chains (for example, concurrent failures in the electricity grid, communications networks, water management and data infrastructure). A significant proportion of recorded cyber incidents are related to service interruptions in the public sector and the energy sector. Tools based on artificial intelligence enable targeted attacks against system-critical nodes (for example, SCADA systems and reserve-management platforms) that can disable entire infrastructure networks. More generally, the increasing dependence of operational resilience on the integrity of information systems means that both physical and digital access to systems constitute threat vectors.

Disinformation campaigns that call into question the competence and legitimacy of the public sector may reduce the population's willingness to follow emergency instructions or may trigger panic and overload the capacity of vital services. Misinformation (for example, that water supplies have been poisoned, that power outages have been covered up, or that important medicines have serious side effects) can lead to irrational consumer behaviour that destabilises the planning and operation of services. In this regard, even a psychological or informational attack that involves no physical or technical component may cause temporary service interruptions or a crisis of confidence that threatens their continuous provision.

Essential services such as power supply, communications, transport and healthcare have become strategic targets in the context of interstate conflict. The massive cyberattacks observed in Ukraine (for example, NotPetya in 2017 and attacks on energy and communications infrastructure in 2022–2024) demonstrate that state-directed cyber activity can be directly used to exert military pressure via critical infrastructure. In the Estonian context, damage to submarine Baltic cables, gas interconnectors or communications links could interrupt services not for days but for weeks, especially if multiple sectors are affected simultaneously.

Geoeconomic confrontation (for example, between Russia and the EU) also affects the operation of critical infrastructure and essential services. Sanctions and supply restrictions can disrupt supply chains for raw materials, spare parts or technological components that are necessary to maintain and develop infrastructure. Interruptions in deliveries or increases in the prices of imported, component-dependent equipment (for example, high-voltage switchgear, generator parts or medicines) may increase the time between maintenance cycles and raise the risk of outages. Energy infrastructure, medical infrastructure and IT systems are particularly vulnerable when logistics depend on international suppliers and macro-level stability. Ensuring continuity of critical infrastructure requires flexible supply chains and strategic reserves, including domestic reserve capacity.

Social fragmentation and an institutional trust crisis in a polarising society can result in acts of sabotage and related activities (for example, deliberate service blockages or the spread of propaganda that supports sabotage). Service continuity often depends on social cooperation and norms in both normal and crisis conditions (for example, adherence to evacuation orders and restraint in consumption habits), which polarisation undermines. Radicalised individuals or groups may target symbolic or publicly visible infrastructure assets that embody state authority. Consequently, protection of critical infrastructure should encompass not only technical security but also societal resilience, community trust and proactive communication.

Combined impacts and cascade effects affecting critical infrastructure and essential services may occur via cyberattacks coinciding with failures in communications, energy and water supplies. This can have a widespread impact on societal functioning. Unprotected information and data infrastructure create vulnerabilities to threats that can incapacitate state management and operational decision-making in key sectors. Additionally, the growing dependence on private providers (for example, for cloud services and communications) requires these entities to both want and be able to ensure continuity if essential services are not to be held hostage to market risks or geopolitical conflicts.

Recommendations for managing internal security risks over the next five years:

- Ensure layered protection for essential services, covering both physical and digital security.
- Develop mechanisms to secure autonomy and duplication of key services.
- Ensure that cybersecurity specialists are always available and cyber-crisis plans are up to date.
- Establish operational risk-coordination mechanisms with private-sector partners, especially those involved in communications, energy and data infrastructure.

CIVIL PROTECTION AND COMMUNITY CRISIS PREPAREDNESS

As noted above, cyber espionage and cyberattacks can incapacitate vital infrastructure such as energy supplies, communications networks and data repositories. Such disruptions directly affect the physical security of the population and the ability to respond to crises. Cyber incidents may lead to information leaks and unauthorised modification and interruption of systems and services. These, in turn, slow emergency responses and compromise the capacity of civil protection measures. From the perspective of community crisis-preparedness, trust in e-government and digital communication channels may decrease if people experience service interruptions or suspect data breaches. The digi-

tal vulnerability of individuals increases the risk that community networks will be uninformed during a crisis or will receive manipulated information, both of which reduce society's capacity to adapt in a crisis.

The impact of misinformation and disinformation on civil protection and community preparedness is grounded in how the spread of systemic falsehoods – including deepfakes and manipulated narratives – undermines official crisis-notification mechanisms that are critical for civil protection. The targets of disinformation are often Russian-speaking communities and young people, who may be the object of large-scale influence operations in digital environments. In a crisis, misinformation may also generate uneven perceptions of risk, as a result of which different communities may respond differently to or fail to follow official guidance.

The war in Ukraine has shown that infrastructure intended to protect the population – for example, shelters, evacuation plans and communications networks – are natural targets. For Estonia, this implies the need to restore and test a variety of sheltering capabilities, maintain distributed crisis reserves and conduct realistic community-level exercises. The war has heightened tensions and fear in communities, especially where there are national and ideological divisions. This may impede trust-based cooperation in crisis situations. At the same time, the war has spurred an increase in community solidarity and greater crisis preparedness.

The impact of the geoeconomic confrontation with Russia may affect civil protection when Russian influence activities disrupt EU internal supply chains or supply chains between Member States and partners. This can create uncertainty or shortages in medicines, fuel or food. Communities and groups that are already socio-economically vulnerable – for example, residents of peripheral areas, older people, or single parents – may lose focus on crisis-preparedness, as immediate survival needs take up all attention. These difficulties can widen feelings of estrangement from state and security structures and reduce people's willingness to cooperate in a crisis.

Societal polarisation in Estonia, including ideological and values-based divisions, may affect civil protection if official threat notifications and crisis information are interpreted from ideological perspectives. This can lead to a situation where segments of the population may refuse to accept official guidance or actively oppose it, as occurred during the COVID-19 pandemic. Misinformation and the activities of extremist groups can disrupt evacuations, cooperation with local authorities and emergency management. Echo chambers and conspiracy theories on social media erode community cohesion and prevent shared understandings of threats and responsibilities. Early exposure of young people to extremist material on platforms such as TikTok, Discord and Telegram increases the spread of violent ideologies and social conflicts, which may become a source of risk during crises.

The simultaneous occurrence of multiple crises – for example, large-scale misinformation, energy outages and migration flows – can very quickly make communities highly vulnerable. Political and institutional trust deficits can inhibit crisis communication and resilience. A failure in crisis communication can, in turn, trigger radicalisation and social polarisation.

Recommendations for managing internal security risks over the next five years:

- Develop integrated civil-protection strategies for multi-crisis scenarios.
- Under a comprehensive national defence approach, strengthen community preparedness with a clear division of societal roles and enhanced social cohesion.

- Incorporate the psychology of information consumption and digital literacy measures into crisis-notification planning.

SOCIETAL SECURITY

Hostile state or organised actors use systemic cyberattacks to target social services, identity-management systems and financial infrastructure. Such attacks can cause service interruptions and personal-data leaks, which in turn undermine people's sense of security and trust in the state's capacity to protect them. Cyberattacks that disrupt benefits payments, medical records databases or the population register, for example, may create inequalities and social stress, especially among vulnerable groups such as older people and persons with disabilities.

Misinformation and disinformation also affect societal security. The systemic spread of false information produces competing interpretations of social problems, erodes social cohesion and encourages group-based stigmatisation. Narratives that portray state institutions as corrupt or falsely present particular social groups as threats can lead to opposing camps of opinion and fuel mutual hostility between them. For example, the deliberate spread of anti-Estonia narratives in the Russian-speaking population in Ida-Viru county may inflame local conflicts, especially if they find support in local communities and online forums.

The continuation of the war in Ukraine, the graphic and emotive media coverage and the slow progress of liberation have eroded public morale and psychological resilience, particularly among lower-income groups for whom day-to-day survival has become an ever-present concern. Escalation in Ukraine can reduce the sense of security and in some cases cause psychosocial stress that manifests as hostile behaviour or hate speech (see also Kaitsepolitseiamet, 2024, 2025).

Geoeconomic confrontation raises prices and reduces purchasing power, which makes it difficult for low-income households to acquire basic necessities and access essential services. When increases in the cost of living become visible and are rooted in complex or geopolitical causes, dissatisfaction is often projected onto domestic politics or particular population groups, which further increases social tension. Areas with high unemployment and high rates of single parenthood, unemployed people and older persons are at particular risk of rapid deterioration in living standards during economic contraction or supply-chain disruption.

Societal polarisation – for example, the widening of ideological divides between liberals and conservative values or those with nationalist and globalist outlooks – fractures the social environment and reduces mutual trust and the willingness to cooperate. While viewpoint-based polarisation in Estonia has generally remained peaceful, disputes over vaccination, refugees, the war in Ukraine, the green transition or education can nevertheless become low-intensity conflicts in workplaces, educational institutions and community networks. The vulnerability of children and young people is particularly critical since they are exposed to polarising and radicalising content at an early age, which can lead to a decrease in trust in social institutions or an increase in exclusion and violence.

Cascade effects among threats to societal security – for example, misinformation, unemployment, economic hardship and identity crises – can provoke social tensions and even mass unrest, especially during economic downturns or geopolitical crises. The radicalisation of young people through social media and poorly moderated platforms can foster

violent extremism. Social division and antagonism between groups becomes a security problem to the extent that it threatens the constitutional order.

Recommendations for managing societal-security risks over the next five years:

- Develop a long-term societal resilience strategy to reduce societal fragmentation.
- Increase public awareness and establish targeted intervention mechanisms for at-risk groups, including in the digital domain.
- Strengthen the legitimacy and increase the inclusiveness of democratic institutions through reliable crisis communication and civic education.

POTENTIAL IMPACT ON ESTONIA'S INTERNAL SECURITY OF MULTIPLE RISKS MATERIALISING SIMULTANEOUSLY

The foregoing discussion demonstrates that the simultaneous realisation of multiple risks can affect all four focus domains (border security; critical infrastructure and essential services; civil protection and community crisis preparedness; and societal security) in distinctive ways and more extensively than the realisation of any single risk in isolation. A possible synergistic multi-crisis – for example, a combination of cyber warfare, misinformation, migration pressure and economic instability – may affect all focus domains at once.

To illustrate this, a hypothetical scenario can be constructed in which several different crises occur in Estonia simultaneously, some of which are deliberately triggered by an external interest group. In this scenario, a cyberattack organised and supported by a hostile foreign state temporarily incapacitates communications and energy infrastructure, including border-surveillance systems and data-management services. At the same time, a misinformation campaign spreads that presents the crisis as a staged event by the Estonian government to secure greater public compliance and that calls for civil disobedience. Additionally, an armed conflict in the Middle East has produced significant migration pressure on the EU's eastern borders. Finally, escalating geopolitical tensions between Asia and the West are disrupting supply chains and causing price rises and shortages of goods.

In this scenario, the four focus domains might be affected in the following ways:

- Border security: As a result of the cyberattacks, some electronic surveillance systems on the eastern border and document-control systems at the eastern border and at Tallinn airport cease to function during severe winter freezing or a summer heatwave. This causes confusion in the management of border crossings and additional delays in border processing. Disinformation asserting that Estonia's border is open or that crossings have been suspended provokes unrest in border communities and distrust of border authorities. At the same time, the escalating migration pressure and presence of large numbers of demographically vulnerable groups from third countries (children, older people) in the area between Russian and Estonian crossing points or along the green border increases the strain on reception capacity and the ability to manage incoming traffic. This compromises the operational functioning of the police and border guard, even more so if the tax and customs authority lacks supporting capacity on site and cooperation with communities is weak. As the situation escalates, border regions fall under the sway of a contradictory and manipulative information campaign, which diminishes institutional authority.

- Infrastructure and services: Targeted attacks on energy and communications systems reduce access to essential services across the country (for example, communications between emergency dispatch centres and healthcare facilities are disrupted and payment terminals stop working). The interruption of cloud-based services (for example, e-prescriptions, the population register) and the risk of data loss disables logistics and supply chains. A supply crisis (for example, shortages of medicines or spare parts) forces the closure of some primary healthcare services, increasing vulnerability. Services are temporarily reallocated to meet priorities, engendering dissatisfaction and the perception of inequality across regions.
- Civil protection and crisis preparedness: Organised misinformation spread by hostile organisations or by a foreign state maligning crisis mismanagement – for example, "the government is hiding the truth" or "the temporary evacuation is a trap" – undermines the population's willingness to follow crisis-management instructions. Communications channels disrupted by cyberattacks impede emergency communication, including the operation of sirens and SMS-alert systems. Local crisis reserves (for example, food distribution and sheltering capacity) prove insufficient because planning did not account for a multi-crisis scenario. Reduced trust in public authorities causes people to turn to unreliable sources and radicalised networks, damaging social cohesion at the community level.
- Societal security: Shortages of critical goods resulting from supply-chain disruption trigger unrest in communities receptive to Russian disinformation narratives and provoke protests directed by hostile actors, amplified by extremist narratives on social media. Misinformation and disinformation portray particular national groups or officials as enemies, further generating social tension and polarisation. Economically vulnerable groups bear a disproportionate share of the crisis burden, deepening perceived injustice and fuelling social conflict. Trust in social-protection systems declines.

Although such a scenario is largely hypothetical, it illustrates the potential interaction of geopolitical tensions, technological threats and social problems in the coming years. In the Estonian context, this shows that crisis preparedness must not rely on linear risk management but requires systemic, strategically planned approaches that account for cross-dependencies. Strengthening the continuity of essential services, community resilience and communicative resilience is imperative if Estonian society is to remain stable under complex security shocks. The resilience of Estonia's internal security depends on crisis resolution measures that rely on integrated and predictive risk management, not isolated response capacities. Therefore, it is advisable to move towards a foresight-driven, adaptive and broad-based security posture in which technology, social cohesion and trust in institutions mutually reinforce one another.

SUMMARY

The key to risk management is the capacity to anticipate possible future scenarios, and science has a central role in this. It is also important to acknowledge that scientific and technological breakthroughs alone are not sufficient to overcome contemporary crises. It is essential to learn from every crisis and treat those lessons as opportunities to support societal change, maintaining that effort even when immediate threats are absent.

In situations where public pressure demands rapid political intervention, the need to justify decisions through a scientific approach increases – particularly when measures are unpopular, enjoy limited public support or their effects are not immediately visible. At the same time, it must be emphasised that science can offer only informed options for action, while responsibility for final decisions rests with political decision makers. Even in crises, it is important to distinguish these roles clearly and to ensure public understanding of transparent and trusted cooperation between scientists and politicians.

According to Estonian subject-matter experts, the global risks judged most likely to affect Estonia's internal security in 2026–2030 are:

- cyber espionage and warfare;
- the spread of misinformation and disinformation;
- interstate armed conflicts;
- geoeconomic confrontation;
- societal polarisation.

At the same time, the experts considered both a shortage of talent and skilled labour and disruptions to critical infrastructure and key supply chains to be likely scenarios. A shortage of skilled workers would threaten not only the technology sector but also the state's capacity to manage emerging risks, in particular performing functions essential to internal security if multiple vital services are simultaneously impaired. It is also important to pay greater attention to the risks arising from supply-chain disruptions and the necessity of securing reserves to guarantee societal functioning.

The rapid development of artificial intelligence, especially generative AI, increases the complexity of cyber espionage and cyberattacks. Concurrently, the vulnerability of critical infrastructure is deepening. Estonia recorded a record number of high-impact cyber incidents in 2024. AI-based manipulation techniques (for example, deepfakes) increase public distrust of democratic institutions and intensify social fragmentation. Young people are particularly at risk when using social media and unregulated information environments. In the present, technological development and hybrid threats (including misinformation, populism and extremism) are already widening the divisions between

communities, while at the same time, both political decision-making and public trust are under threat.

Russia's aggression in Ukraine, and tensions in the Middle East and Asia, may cause escalating migration pressure, increased terrorism risk and social destabilisation in Estonia. The risk of radicalisation is also growing and is closely connected to global conflicts. Estonia's economy is vulnerable to the effects of a US–China trade confrontation.

The concurrent realisation of multiple risks – in other words, multi-crises – is likely and may overload standard crisis-management mechanisms. Particularly severe consequences can arise if access to information, energy and critical services is disrupted simultaneously. To conclude, to increase strategic readiness, it is necessary to strengthen broad-based national defence, develop public cyber hygiene and critical thinking about information, increase investment in the training of cybersecurity specialists, and reduce dependence on unstable supply chains.

The study offers the following recommendations for policy-makers.

- Integrate evidence-based forecasts into crisis management and strategic planning.
- Increase investment in cybersecurity, cyber awareness and counter-drone measures.
- Create additional mechanisms to counter the spread of misinformation and to mitigate societal polarisation.
- Ensure multilayered protection for critical infrastructure with particular attention to communications, energy and data networks.
- Systematically monitor the impact of global conflicts on Estonia's internal security and develop predictive methodologies and models accordingly.

REFERENCES

Adlakha, H., 2023. 10 Reasons Xi Won't Attack Taiwan Anytime Soon. The Diplomat, 20 January 2023. [Online] Available at: https://thediplomat.com/2023/01/10-reasons-xi-wont-attack-taiwan-anytime-soon/ [Accessed 13.05.2025].

Altman, H., 2025. "Cartel Members Fought in Ukraine to Learn FPV Drone Skills: Report." *The War Zone*, 30 July 2025. [Online] Available at: https://www.twz.com/news-features/cartel-members-fought-in-ukraine-to-learn-fpv-drone-skills-report [Accessed 22.08.2025].

Anghel, V., 2025. *Global Risks to the EU*. European University Institute. [Online] Available at: https://cadmus.eui.eu/server/api/core/bitstreams/bf016066-0244-5253-9c9a-6229fa318598/content [Accessed 21.03.2025].

Bonifassi, S. & Bastien, J., 2025. *A closer look at EU sanctions enforcement following adoption of new directive*. Global Investigations Review, 30 June 2025. [Online] Available at: https://globalinvestigationsreview.com/guide/the-guide-sanctions/sixth-edition/article/closer-look-eu-sanctions-enforcement-following-adoption-of-new-directive [Accessed 12.09.2025].

Borbáth, E., Hutter, S., & Leininger, A., 2023. Cleavage politics, polarisation and participation in Western Europe. *West European Politics*, Vol. 46(4), pp. 631–651. https://doi. org/10.1080/01402382.2022.2161786

Burgess, S., 2022. Ukraine war: Deepfake video of Zelenskyy telling Ukrainians to 'lay down arms' debunked. SkyNews, 17 March 2022. [Online] Available at: https://news.sky.com/story/ukraine-war-deepfake-video-of-zelenskyy-telling-ukrainians-to-lay-down-arms-debunked-12567789 [Accessed 03.06.2025].

Data Guardian Hub, 2024. How Cyber Espionage Threats Have Evolved: A Look at 5 Key Trends in 2024. Data Guardian Hub, 20 May 2024. [Online] Available at: https://www.es.consulting/blog/cybersecurity-trends-for-2024-a-look-into-the-future [Accessed 03.06.2025].

Deloitte, 2025. Global Cyber Threat Intelligence (CTI). Annual Cyberthreat Trends Report – 2024. [Online] Available at: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-annual-cyber-threat-trends-report-2025.pdf [Accessed 03.06.2025].

DOJ, 2023. Press Release: U.S. Attorney Announces Charges And New Arrest In Connection With Assassination Plot Directed From Iran. Press release, U.S. Attorneys Office, Southern District of New York, U.S Department of Justice. [Online] Available at: https://www.justice.gov/usao-sdny/pr/us-attorney-announces-charges-and-new-arrest-connection-assassination-plot-directed [Accessed 22.08.2025].

Duffy, K. & Harbath, K., 2024. Defending the Year of Democracy: What It Will Take to Defend 2024's 80-Plus Elections From Hostile Actors. *Foreign Affairs,* 04 January 2024. [Online] Available at: https://www.foreignaffairs.com/united-states/defending-year-democracy [Accessed 24.08.2025].

Eesti Vabariigi Välisministeerium, 2025. Euroopa Liit võttis vastu uue sanktsioonipaketi Venemaale. 18 July 2025. [Online] Available at: https://vm.ee/uudised/euroopa-liit-vottis-vastu-uue-sanktsioonipaketi-venemaale [Accessed 12.08.2025].

Edwards, C. & Seidenstein, N., 2025. *The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure.* The International Institute for Strategic Studies, August 2025. [Online] Available at: https://www.iiss.org/research-paper/2025/08/the-scale-of-russian--sabotage-operations--against-europes-critical--infrastructure/ [Accessed 12.09.2025].

Euroopa Parlamendi ja nõukogu direktiiv (EL) 2024/1226, 24 April 2024, mis käsitleb liidu piiravate meetmete rikkumisega seotud kuritegude määratlemist ja nende eest mõistetavaid karistusi ning millega muudetakse direktiivi (EL) 2018/1673. ELT L, 2024/1226, 29.4.2024.

European Commission, 2024a. Eurobarometer 547. Cyberskills. [Online] Available at: https://europa.eu/eurobarometer/surveys/detail/3176 [Accessed 03.06.2025].

European Commission, 2024b. Eurobarometer 547. Cyberskills. Facktsheet – Estonia. [Online] Available at: https://europa.eu/eurobarometer/api/deliverable/download/file?deliverableId=93205 [Accessed 03.06.2025].

Europol SOCTA, 2025. Europol, *European Union Serious and Organised Crime Threat Assessment – The changing DNA of serious and organised crime*, Publications Office of the European Union, Luxembourg, 2025. [Online] Available at: https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf [Accessed 22.08.2025].

Europol TESAT, 2024. *European Union Terrorism Situation and Trend Report 2024*, Luxembourg: Publications Office of the European Union. [Online] Available at: https://www.europol.europa.eu/cms/sites/default/files/documents/TE-SAT%202024.pdf [Accessed 22.08.2025].

Europol TESAT, 2025. European Union Terrorism Situation and Trend Report 2025, Luxembourg: Publications Office of the European Union. [Online] Available at: https://www.europol.europa.eu/cms/sites/default/files/documents/EU_TE-SAT_2025.pdf [Accessed 22.08.2025].

GTI, 2025. *Global Terrorism Index 2025: Measuring The Impact of Terrorism,* Sydney: Institute for Economics & Peace. [Online] Available at: https://www.visionofhumanity.org/wp-content/uploads/2025/03/Global-Terrorism-Index-2025.pdf [Accessed 22.08.2025].

Hambling, D., 2025. "Moving Targets: Implications of the Russo-Ukrainian War for Drone Terrorism." *CTC Sentinel Combating Terrorism Center at West Point* 18 (7). [Online] Available at: https://ctc.westpoint.edu/wp-content/uploads/2025/07/CTC-SENTINEL-072025_cover-article.pdf [Accessed 22.08.2025].

Hitachi Cyber, 2025. Cyber Threat Landscape in 2025: Trends and Challenges. [Online] Available at: https://hitachicyber.com/cyber-threat-landscape-in-2025-trends-and-challenges/ [Accessed 21.05.2025].

Höller, L., 2025. Drug cartel operatives snuck into Ukraine for drone training: report. Defence News, 30 July 2025. [Online] Available at: https://www.defensenews.com/global/the-americas/2025/07/30/drug-cartel-operatives-snuck-into-ukraine-for-drone-training-report/ [Accessed 22.08.2025].

ISCP, 2025. Intelligence and Security Committee of Parliament. Iran. HC 1116. London: UK Parliament. [Online] Available at: https://isc.independent.gov.uk/wp-content/uploads/2025/07/Intelligence-and-Security-Committee-of-Parliament-Iran.pdf [Accessed 22.08.2025].

Jones, Seth G., 2025. Russia's Shadow War Against the West. CSIS Briefs. March. Center for Strategic and International Studies. [Online] Available at: https://www.csis.org/analysis/russias-shadow-war-against-west [Accessed 22.08.2025].

Joske, A., 2022. Spies and Lies. How China's Greatest Covert Operation Fooled the World. Berkeley, CA: Hardie Grant Books.

Jüris, F., 2023. Making friends, making inroads: The CCP's influence activities in Estonia. Sinopsis. Aca Media. [Online] Available at: https://sinopsis.cz/en/making-friends-making-inroads-the-ccps-influence-activities-in-estonia/ [Accessed 24.07.2025].

Kaitsepolitseiamet, 2024. Aastaraamat 2023-2024. [Online] Available at: https://kapo.ee/sites/default/files/content_page_attachments/Aastaraamat%202023-2024.pdf [Accessed 14.05.2025].

Kaitsepolitseiamet, 2025. Kaitsepolitsei aastaraamat 2024-2025. Tallinn: Kaitsepolitseiamet. [Online] Available at: https://kapo.ee/sites/default/files/content_page_attachments/aastaraamat-2024-2025_0.pdf [Accessed 25.04.2025].

Kaljula, R., 2024. Väike Taiwan – tehnoloogiline suurriik. Postimees AK, 13 January 2024. [Online] Available at: https://maailm.postimees.ee/7936785/ak-vaike-taiwan-tehnoloogiline-suurriik [Accessed 14.05.2025].

Karistusseadustik. RT I, 05.07.2025, 9.

Kantrowitz, A., 2025. AIs Deceive Human Evaluators. And We're Probably Not Freaking Out Enough. CMSWire, 27 February 2025. [Online] Available at: https://www.cmswire.com/ai-technology/ais-deceive-human-evaluators-and-were-probably-not-freaking-out-enough/ [Accessed 12.09.2025].

Kubin, E. & von Sikorski, C., 2021. The role of (social) media in political polarization: a systematic review. *Annals of the International Communication Association*, *45*(3), pp. 188–206. https://doi.org/10.1080/23808985.2021.1976070

Läänemets, M., 2022. Miks Hiina pelgab Taiwanit rünnata? Postimees, 28 July 2022. [Online] Available at: https://arvamus.postimees.ee/7572702/mart-laanemets-miks-hiina-pelgab-taiwanit-runnata [Accessed 13.05.2025].

Läänemets, M., 2023. Russo-Ukrainian war and China's global interests. *Security Spectrum. Proceedings of the Academy of Security Science*s, 22, pp. 177–189. [Online] Available at: https://digiriiul.sisekaitse.ee/handle/123456789/3154 [Accessed 14.05.2025].

Läänemets, M., 2024. Hiina „suur plaan" ja selle mõju Eesti julgeolekule. Turvalisuskompass, 7 (2), pp. 9–32.

Loik, R., 2022. Venemaa „infomürsud" Ukraina vastu valmistasid ette konventsionaalset kallaletungi. Diplomaatia, No. 211, pp. 16–20. [Online] Available

at: https://diplomaatia.ee/venemaa-infomursud-ukraina-vastu-valmistasid-ette-konventsionaalset-kallaletungi/ [Accessed 16.05.2025].

Loik, R., 2024. Undersea Hybrid Threats in Strategic Competition: The Emerging Domain of NATO–EU Defense Cooperation. Journal on Baltic Security, 10 (2), pp. 1–25. [Online] Available at: https://journalonbalticsecurity.com/journal/JOBS/article/126/text [Accessed 24.08.2025].

Lomp, L-E., 2025. Peeter Tali: Kohtla-Järve sotsidest juhid on poliitiliselt kurdid ja pimedad. Postimees, 28 January 2025. [Online] Available at: https://www.postimees.ee/8181083/peeter-tali-kohtla-jarve-sotsidest-juhid-on-poliitiliselt-kurdid-ja-pimedad [Accessed 24.07.2025].

Madsen, T., 2024. Hiina suursaadik parlamendiliikmete visiidist: ma ei nõustu sõnaga «skandaal». Postimees, 19 December 2024. [Online] Available at: https://www.postimees.ee/8155755/intervjuu-hiina-suursaadik-parlamendiliikmete-visiidist-ma-ei-noustu-sonaga-skandaal [Accessed 24.07.2025].

Mahmudov, N., 2023. Cyber warfare: understanding the elements, effects, and future trends of cyber-attacks and defences. Security & Defense, 2, pp. 37–54.

Manak, I., Patterson, R., Liu, Z., O'Neil, S.K., Setser, B.W., Alden, E., Steil, B., Hillman, J.E., Goodman, M.P., & Freeman, W., 2025. What Trump Trade Policy Has Achieved Since 'Liberation Day'. Greenberg Center for Geoeconomic Studies at the Council on Foreign Relations. [Online] Available at: https://www.cfr.org/article/what-trump-trade-policy-has-achieved-liberation-day [Accessed 12.08.2025].

Marcus, G. & Hamiel, N., 2024. LLMs + Coding Agents = Security Nightmare. *Marcus on AI*, 17 August 2025. [Online] Available at: https://garymarcus.substack.com/p/llms-coding-agents-security-nightmare [Accessed 12.09.2025].

Muuga, E., Loik, R., Kaup, G.-H., Savimaa, R., & Koort, E. 2025. Julgeolekuohud Balti riikide merealuste ühendustega seotud kriitilisele taristule: Läänemeri hübriidsõja tulipunktis. Tallinn: Sisekaitseakadeemia. [Online] Available at: https://digiriiul.sisekaitse.ee/handle/123456789/3579 [Accessed 16.05.2025].

O'Donnell, J., Heaven, W. O., & Heikkilä, M., 2025. What's next for AI in 2025. MIT Technology Review, 08 January 2025. [Online] Available at: https://www.technologyreview.com/2025/01/08/1109188/whats-next-for-ai-in-2025/ [Accessed 03.06.2025].

OECD, 2023. *OECD Digital Education Outlook 2023: Towards an Effective Digital Education Ecosystem*, OECD Publishing, Paris. https://doi.org/10.1787/c74f03de-en

Pickle, C., 2024. The Changing Character of Cyber Warfare. U.S. Naval Institute Proceedings, 150/6/1456. [Online] Available at: https://www.usni.org/magazines/proceedings/2024/june/changing-character-cyber-warfare [Accessed 03.06.2025].

PST, 2025. Norwegian Police Security Service (PST). National Threat Assessment 2025. Oslo: Politiets Sikkerhetstjeneste. [Online] Available at: https://www.pst.no/globalassets/2025/nasjonal-trusselvurdering-2025/_nasjonal-trusselvurdering-2025_uu-engelsk.pdf [Accessed 22.08.2025].

Puri, S., 2025. *President Trump's tariffs increase pressure on allies to reduce security dependence on the US*. Chatham House, 15 April 2025. [Online] Available at: https://www.chathamhouse.org/2025/04/president-trumps-tariffs-increase-pressure-allies-reduce-security-dependence-us [Accessed 12.08.2025].

Rassler, D. & Veilleux-Lepage, Y., 2025. "On the Horizon: The Ukraine War and the Evolving Threat of Drone Terrorism" *CTC Sentinel Combating Terrorism Center at West Point 18 (3).* [Online] Available at: https://ctc.westpoint.edu/wp-content/uploads/2025/03/CTC-SENTINEL-032025_cover-article.pdf [Accessed 22.08.2025].

Riigi Infosüsteemi Amet, 2025. *Küberturvalisuse aastaraamat 2025*. [Online] Available at: https://www.ria.ee/kuberturvalisuse-aastaraamat-2025 [Accessed 16.05.2025].

Rohac, D., 2024. Chinese Influence in Central and Eastern Europe. American Enterprise Institute, 11 September 2024. [Online] Available at: https://www.aei.org/wp-content/uploads/2024/09/20240906-Testimony-Europe-subcommittee-DR-reviewed-final-edits-1.pdf?x85095 [Accessed 24.07.2025].

Roy, D., 2024. Why China remains unlikely to invade Taiwan. The Lowy Institute, 17 April 2024. [Online] Available at: https://www.lowyinstitute.org/the-interpreter/why-china-remains-unlikely-invade-taiwan [Accessed 13.05.2025].

Savimaa, R. & Loik, R., 2023. Kogemused Eesti siseturvalisusele 2022. aastal Ukrainale konventsionaalset jätkuinvasiooni ettevalmistavast faasist. Tallinn: Sisekaitseakadeemia. [Online] Available at: https://digiriiul.sisekaitse.ee/handle/123456789/2990 [Accessed 16.05.2025].

Savimaa, R., Puusalu, J., Loik, R., Ringvee, R., Läänemets, M., Tammel, K., Kont, K-R., & Saar, J., 2024. *Sisejulgeoleku väliskeskkonna trendid ja prognoos*. Sisekaitseakadeemia. [Online] Available at: https://doi.org/10.15158/kkn4-nd47 [Accessed 15.03.2025].

Schroeder, D. T. et al., 2025. "How Malicious AI Swarms Can Threaten Democracy". https://doi.org/10.48550/arXiv.2506.06299

Serani, D., 2025. Affective polarization, political mistrust and populist attitudes: longitudinal evidence from Italy. *Contemporary Italian Politics*, pp. 1–22. https://doi.org/10. 1080/23248823.2025.2475631

Shin, D. & Jitkajornwanich, K., 2024. How Algorithms Promote Self-Radicalization: Audit of TikTok's Algorithm Using a Reverse Engineering Method. *Social Science Computer Review,* Vol. 42 (4), pp. 1020–1040. https://doi.org/10.1177/08944393231225547

Suzan, S. & Bounfour, A., 2023. New oil map: Impact of Russia's war on Ukraine on supply and demand. European Federation for Transport and Environment AISBL. [Online] Available at: https://www.transportenvironment.org/uploads/files/202307_oil_imports_report_compressed.pdf [Accessed 12.08.2025].

Taylor, M., 2024. An AI Deepfake Could Be This Election's November Surprise. Time, 03 October 2024. [Online] Available at: https://time.com/7033256/ai-deepfakes-us-election-essay/ [Accessed 03.06.2025].

Välisluureamet, 2024. Eesti rahvusvahelises julgeolekukeskkonnas 2024. [Online] Available at: https://www.valisluureamet.ee/doc/raport/2024-et.pdf [Accessed 13.05.2025].

Välisluureamet, 2025. Eesti rahvusvahelises julgeolekukeskkonnas 2025. Tallinn: Välisluureamet. [Online] Available at: https://www.valisluureamet.ee/doc/raport/2025-et.pdf [Accessed 12.04.2025].

Vlassov, J., 2025. The Iron House: Geopolitical Stakes of the US-China AGI Race. [Online] Available at: https://www.convergenceanalysis.org/fellowships/

international-security/the-iron-house-geopolitical-stakes-of-the-us-china-agi-race [Accessed 12.09.2025].

Walsh, N. P., 2025. China tells EU it can't accept Russia losing its war against Ukraine, official says. CNN, 04 July 2025. [Online] Available at: https://edition.cnn.com/2025/07/04/europe/china-ukraine-eu-war-intl [Accessed 12.09.2025].

World Economic Forum, 2020. *The Global Risks Report 2020*. [Online] Available at: https://www.weforum.org/publications/global-risks-report-2020 [Accessed 21.02.2025].

World Economic Forum, 2024. *The Global Risks Report 2024*. [Online] Available at: https://www.weforum.org/publications/global-risks-report-2024 [Accessed 21.02.2025].

World Economic Forum, 2025. Global Cybersecurity Outlook 2025. [Online] Available at: https://www.weforum.org/publications/global-cybersecurity-outlook-2025/ [Accessed 03.06.2025].

World Economic Forum, 2025. *The Global Risks Report 2025*. [Online] Available at: https://www.weforum.org/publications/global-risks-report-2025 [Accessed 21.02.2025].

Yarchi, M., Baden, C., & Kligler-Vilenchik, N., 2020. Political Polarization on the Digital Sphere: A Cross-platform, Over-time Analysis of Interactional, Positional, and Affective Polarization on Social Media. *Political Communication*, Vol. 38(1–2), pp. 98–139. https://doi.org/10.1080/10584609.2020.1785067

Zandee, D., van der Meer, S., & Stoetman, A., 2022. Countering Hybrid Threats: Steps for Improving EU-NATO cooperation. Clingendael Report. Netherlands Institute of International Relations. [Online] Available at: https://www.clingendael.org/pub/2021/countering-hybrid-threats/ [Accessed 24.08.2025].

Zygar, M., 2024. "Russia's War on Woke: Putin Is Trying to Unite the Far Right and Undermine the West." Foreign Affairs, 02 January 2024. [Online] Available at: https://www.foreignaffairs.com/russian-federation/russias-war-woke [Accessed 24.08.2025].

APPENDICES

APPENDIX 1. METHODOLOGY

When compiling the overview of development trends (to 2030) the substantial uncertainty inherent in long-range forecasting was taken into account, and four additional measures were combined to ensure the quality of the analysis: a discussion-based working process (including a subject-matter expert survey), use of recognised forecasts as inputs, differentiation of categories, and an assessment of the likelihood of risk materialisation.

The primary basis of this study is the World Economic Forum's Global Risk Perception Survey (GRPS) (Global Risks Report, 2024) risk assessment across five principal domains, supplemented by impact assessments from the European University Institute's document Global Risks to the EU 2025, the potential implications of which for Estonia were evaluated separately. To develop as accurate a composite picture as possible of risks and their potential impacts, an additional survey was conducted to assess impacts; respondents were Estonian experts from a cross-section of relevant fields. Experts were selected to include specialists with knowledge of environmental, technological, economic, social science and geopolitical issues. Using a purposive sample, 24 Estonian subject-matter experts from academia, the private sector and the public sector assessed, in April 2025, 29 pre-identified global risks on two dimensions: the likelihood of risk materialisation and the expected impact on Estonia over a 5–7-year horizon. Environmental risks and the probability of their realisation were additionally assessed for a 10–50-year horizon.

The 29 identified risks were grouped into the following domains (see Appendix 2 for details):

- social and societal risks
- economic risks
- geopolitical risks
- environmental risk factors
- technological risks

For each domain, the probability of trends/risks materialising and their potential impact on Estonia were assessed on the following scale:

MINIMAL	LOW	MODERATE	HIGH	VERY HIGH

When presenting trends by domain, emphasis was placed primarily on aspects that affect national internal security, and the report describes in greater detail the assessment results for the five global risks rated potentially to have the largest impact on Estonia.

APPENDIX 2. DEFINITIONS OF GLOBAL RISKS

(according to the Global Risk Perception Survey 2024)

SOCIETAL RISKS

Decline in health and well-being
Regular or chronic impacts on physical and mental health and well-being that require substantive medical attention and/or limit activities of daily living. Includes, but is not limited to: conditions linked to ageing, excessive consumption habits, and climate change (including heatwaves) and pollution.

Erosion of human rights and/or civic freedoms
Loss of protections for rights inherent to all human beings, regardless of individual status, and/or the freedoms that underpin civic space. Includes, but is not limited to, the right to: life and liberty; work and education; freedom of expression; peaceful assembly; non-discrimination based on gender, race, ethnicity and other characteristics; and privacy.

Inequality (wealth, income)
Present or perceived substantive disparities in the distribution of assets, wealth or income within or between countries, resulting in material differences in related economic outcomes. Includes, but is not limited to: growing or persistent poverty and economic polarisation.

Infectious diseases
Spread of viruses, parasites, fungi or bacteria leading to a widespread loss of life and economic disruption. Includes, but is not limited to: zoonotic diseases, releases of natural or man-made pathogens, the resurgence of pre-existing diseases due to lower levels of immunity, the rise of antimicrobial resistance, and the impact of climate change and environmental degradation on pathogens and their vectors.

Insufficient public infrastructure and social protections
Non-existent, inadequate or inequitable public infrastructure, services and social protections. Includes, but is not limited to: unaffordable or inadequate social security and benefits, housing, public education, child and elderly care, healthcare, sanitation and transportation systems, and pension systems.

Lack of economic opportunity or unemployment
Structural deterioration of work prospects or standards of work and/or persistent barriers to the realisation of economic potential and security. Includes, but is not limited to: erosion of workers' rights; stagnating wages; rising unemployment and underemployment; displacement due to automation or the green transition; stagnant social mobility; and unequal access to educational, technological and economic opportunities.

Involuntary migration or displacement
Forced movement or displacement across or within borders, stemming from, but not limited to: persistent discrimination and persecution; lack of economic advancement opportunities; human-made disasters; natural disasters and extreme weather events, including the impacts of climate change; and internal or interstate conflict.

Societal polarisation
Present or perceived ideological and cultural divisions within and across communities leading to declining social stability, gridlocks in decision-making, economic disruption and increased political polarisation.

TECHNOLOGICAL RISKS

Adverse outcomes of AI technologies
Intended or unintended negative consequences of advances in AI and related technological capabilities (including Generative AI) on individuals, businesses, ecosystems and/or economies.

Adverse outcomes of frontier technologies (quantum, biotech, geoengineering)
Intended or unintended negative consequences of advances in frontier technologies on individuals, businesses, ecosystems and/or economies. Includes, but is not limited to: brain-computer interfaces, biotechnology, geoengineering and quantum computing.

Censorship and surveillance
Broad and pervasive observation of a place or person and/or suppression of communication, information and ideas, physically or digitally, to the extent that it significantly infringes on human and civil rights (e.g. privacy, freedom of speech and freedom of expression).

Cyber espionage and warfare
Use of cyber weapons and tools by state and non-state actors to gain control over a digital presence, cause operational disruption, and/or compromise or damage an entity's technological and information networks and infrastructure. Includes: defensive and offensive cyber operations that occur during or trigger armed conflict, and cyberattacks that steal classified, sensitive data or intellectual property to gain an advantage.

Misinformation and disinformation
Persistent false information (deliberate or otherwise) widely spread through media networks, shifting public opinion in a significant way towards distrust in facts and authority. Includes, but is not limited to: false, imposter, manipulated and fabricated content.

Online harms
Erosion of protection from and/or prevalence of harmful behaviour that poses a digital threat to the emotional or mental health and well-being of individuals. Includes, but is not limited to: online child sexual abuse, online harassment and cyberbullying.

GEOPOLITICAL RISKS

State-based armed conflict (proxy, civil wars, coups, terrorism, etc.)
Bilateral or multilateral use of force between states and/or between a state and non-state actor(s), often with ideological, political or religious goals, manifesting as war and/or organised, sustained violence. Includes, but is not limited to: hot wars, proxy wars, civil wars, guerrilla warfare, terrorism, genocide and assassinations.

Biological, chemical or nuclear weapons or hazards
Intentional or accidental release of biological, chemical, nuclear or radiological hazards, resulting in loss of life, destruction and/or international crises. Includes, but is not limited to: accidents at or sabotage of biolaboratories, chemical plants and nuclear power plants; and intentional or accidental release of biological, chemical and nuclear weapons.

Geoeconomic confrontation (sanctions, tariffs, investment screening)
Deployment of economic levers by global or regional powers to reshape economic interactions between nations, restricting goods, knowledge, services or technology with the intent of building self-sufficiency, constraining geopolitical rivals and/or consolidating spheres of influence. Includes, but is not limited to: currency measures, investment controls, sanctions, state aid and subsidies, and trade controls.

Intrastate violence (riots, mass shootings, gang violence, etc.)
Use of force that takes place within a country or community that results in loss of life, severe injury or material damage. Includes, but is not limited to: mass shootings as well as crimes threatening or causing physical harm to the community, such as gang violence, gender-based violence and abductions.

ENVIRONMENTAL RISKS

Biodiversity loss and ecosystem collapse
Severe consequences for the environment, humankind and economic activity due to destruction of natural capital stemming from species extinction or reduction, spanning both terrestrial and marine ecosystems.

Critical change to Earth systems
Long-term, potentially irreversible and self-perpetuating changes to critical planetary systems, as a result of breaching a critical climatic or ecological threshold or 'tipping point', at a regional or global level. Includes, but is not limited to: sea level rise from collapsing ice sheets, carbon release from thawing permafrost, and disruption of ocean or atmospheric currents.

Extreme weather events (floods, heatwaves, etc.)
Loss of human life, damage to ecosystems, destruction of property and/or financial loss due to extreme weather events. Includes, but is not limited to: land-based (e.g. wildfires), water-based (e.g. floods), and atmospheric and temperature-related (e.g. heat-waves) events, including those exacerbated by climate change.

Natural resource shortages (food, water)
Supply shortages of food or water for human, industry or ecosystem use, manifesting as food and water insecurity at a local, regional or global level, stemming from, but not limited to: human overexploitation and mismanagement of critical natural resources, climate change (including drought and desertification), and/or a lack of suitable infrastructure.

Non-weather-related natural disasters (earthquakes, volcanoes, tsunamis, solar flares, etc.)
Loss of human life, damage to ecosystems, destruction of property and/or financial loss due to non-weather-related natural disasters. Includes, but is not limited to: land-based (e.g. earthquakes, volcanoes), water-based (e.g. tsunamis) and extra-terrestrial-based (e.g. asteroid strikes and geomagnetic storms) events.

Pollution (air, soil, water, etc.)
Introduction of harmful materials into the air, water and soil stemming from human activity, resulting in impacts to and loss of human life, financial loss and/or damage to ecosystems. Includes, but is not limited to: household and industrial activities; environmental accidents, such as oil spills; and radioactive contamination.

ECONOMIC RISKS

Asset bubble burst
Prices for housing, investment funds, shares and other assets become increasingly disconnected from the real economy, leading to a severe drop in demand and prices. Includes, but is not limited to: cryptocurrencies, housing prices and stock markets.

Concentration of strategic resources and technologies
Concentration of strategically important resources (minerals, materials, technologies) among a small number of individuals, businesses or states that can control access and dictate discretionary pricing.

Crime and illicit economic activity (incl. cyber)
Global proliferation of organised crime or the illicit activities of businesses and individuals that undermine economic advancement and growth, facilitated on both a borderless and digital basis. Includes, but is not limited to: illicit financial flows (e.g. tax evasion, sanctions evasion and money laundering), illicit trade and trafficking (e.g. counterfeiting, human trafficking, wildlife trade and weapons), and cybercrime (including ransomware, data theft and online fraud).

Debt (public, corporate, household)
Corporate, household, or public finances struggle to service debt accumulation, resulting in mass bankruptcies or insolvencies, liquidity crises or defaults and sovereign debt crises.

Disruptions to a systemically important supply chain
Major disruption or collapse of a systemically important global supply chain or industry with an impact on the global economy, financial markets or society leading to an abrupt shock to the supply and demand of systemically important goods and services at a global scale. Includes, but is not limited to: energy, technological hardware, medical supplies, and fast-moving consumer goods.

Disruptions to critical infrastructure
Overload or shutdown of physical and digital infrastructure (including satellites) or services underpinning critical systems, including the internet, telecommunications, public utilities, financial systems or energy, stemming from, but not limited to: cyberattacks, intentional or unintentional physical damage, extreme weather events, and natural disasters.

Economic downturn (recession, stagnation)
Near-zero or slow global growth lasting for several years or a global contraction (recession or depression).

Inflation
Sustained increases in the price of goods and services. Includes the potential for broad sections of the population being unable to maintain current lifestyle with declining purchasing power.

Talent and/or labour shortages
Global, geographical or industry mismatches between labour and skills supply and demand.

THE KEY TO EFFECTIVE RISK MANAGEMENT IS THE CAPACITY TO ANTICIPATE POSSIBLE FUTURE SCENARIOS, AND SCIENCE HAS A VITAL ROLE TO PLAY.

The five-year (2026–2030) forecast of global development trends affecting Estonia's internal security aims to provide evidence-based strategic input for the development of Estonia's internal security policy.

In early 2025, the Research Centre of the Internal Security Institute at the Estonian Academy of Security Sciences conducted a study in which Estonian subject-matter experts assessed the global risks most likely to materialise and their potential impact on Estonia. The assessment focused on a medium-term horizon (5–7 years) and ranked risks by likelihood and by the scale of their potential impact on Estonia. On the basis of the study results, researchers at the Academy provided additional analysis and explanations of the five risks judged likely to have the largest impact and of their possible interactions.

sisekaitse.ee

ISBN 978-9985-67-540-3