Risks

Last updated on 20.11.2025

Table of contents

Cyber threats

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

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

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

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

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

THREATS

- For Estonia and the wider Western world, Russia's war of aggression against Ukraine has significantly increased cyber threats. This has shown that, in addition to supporting kinetic warfare with cyberattacks against critical infrastructure, cyber operations are also widely used as part of hybrid and information warfare. For example, information operations remain a key element of Russia's war of aggression against Ukraine in the cyber domain. Manipulation of information has intensified, likely also because 2024 saw several major events, particularly elections.

- The threat of supply chain attacks has grown, with attackers compromising software or hardware components embedded in many products. This allows them to gain access to large numbers of organisations worldwide. Attacks through service providers have also become more frequent; for example, compromising a company that provides IT support or accounting services may give criminals access to multiple client networks.

- Security risks are also increased due to technology from third countries in critical infrastructure. Hardware manufacturers or software developers from states hostile to the West may not always be reliable or well-intentioned. Therefore, when using technology originating from third countries, it is necessary to critically assess the associated risks, plan ways to mitigate them, and/or consider alternative options.

- In 2024, the number of impactful cyber incidents in Estonia nearly doubled compared with the previous year, rising from 3,314 to 6,515 (a consistent increase in recent years). These mostly involve cases where individuals, institutions, and companies have lost money or data, and information systems have failed due to cyberattacks or technical faults.

- The incidents that most affect Estonian citizens daily are mass attacks, such as various phishing schemes and fraud (two-thirds of impactful incidents). The sharp increase is largely due to cybercriminals' widespread adoption of artificial intelligence and other automated tools. Using AI for data analysis and natural language processing enables more convincing and personalised fraudulent messages. It also allows attacks to be carried out more quickly and on a larger scale, making them harder to detect and stop. According to Police and Border Guard Board (PPA) data, Estonian individuals and companies lost nearly 8 million euros in 2024 as a result of various fraud schemes – an average of 22,000 euros per day. Risks associated with autonomous superintelligence also need to be considered, including people's limited ability to control and direct its behaviour. The further development of artificial intelligence may create new, previously unknown risks and amplify existing ones, making their mitigation a continuous process.

- The scale and number of denial-of-service attacks grew significantly in 2024. For instance, in one wave of attacks by Russian hacktivist groups, nearly three billion malicious requests were directed against Estonian public sector websites in just four hours – under normal conditions, such a volume would have taken more than 25 years to accumulate. Denial-of-service attacks targeting Estonia are mostly politically motivated and often focus on services whose disruption would affect the largest number of people. Due to geopolitical tensions, more denial-of-service attacks can be expected in the coming years. Attackers are increasingly targeting internet components critical to overall

- functioning, such as name servers, cloud services, and authentication services, on which many other web services depend.

ACTIONS

- Protecting critical infrastructure and vital services has been the focus of Estonia's cybersecurity efforts in recent years, to ensure that basic needs are met – that electricity, data communication, heating, food, and water remain available, and that hospitals and schools continue to function. The state has helped companies test the security of their systems and has provided training and exercises for their employees. A unique cyber reserve has been created, made up of experts from state IT agencies and the Cyber Unit of the Defence League.

- Estonia has contributed to creating a safer environment by establishing an Estonian-language security standard (E-ITS), by informing companies about prevalent cyber threats, and by providing training and assistance in incident management. The implementation of information security standards (such as E-ITS or the international ISO27001) helps ensure that a company maintains a suitable level of information security, service continuity, and a good reputation.

- Cooperation towards a common goal between individuals, institutions, and businesses enables Estonia to respond to cyber threats quickly and flexibly. Our e-services form a network that includes both the public and private sectors, and their security and reliability often depend on one another. Service owners must identify these interdependencies and comply with security requirements throughout the entire lifecycle of their products or services.

Expand all

Read more

Cyber Security in Estonia 2025 – Information System Authority

Last updated on 11.11.2025