The Hague Centre
for Strategic Studies

Guest Paper

Estonia's Preparedness to Counter Russian Hybrid Threats

Marek Kohv

November 2026





The Hague Centre
for Strategic Studies

Estonia's Preparedness to Counter Russian Hybrid Threats

Guest Paper

Author:
Marek Kohv

Quality Assurance:
Davis Ellison and Hans Horan

The cover image was AI-generated.

November 2026

The research for and production of this report has been conducted within the PROGRESS research framework agreement. Responsibility for the contents and for the opinions expressed, rests solely with the authors and does not constitute, not should be construed as, an endorsement by the Netherlands Ministries of Foreign Affairs and Defence.

This publication is **AI-supported***.

© *The Hague* Centre for Strategic Studies. All rights reserved. No part of this report may be reproduced and/or published in any form by print, photo print, microfilm or any other means without prior written permission from HCSS. All images are subject to the licenses of their respective owners.

* AI was used to assist with brainstorming, structuring ideas, reviewing arguments, identifying blind spots, and/or improving clarity. Core analytical tasks such as literature review, conceptual development, substantive judgement and final writing remain human led. The authors take full responsibility for the integrity of the work.

Introduction

Estonia's preparedness to counter hybrid threats rests on cooperation among state institutions and society's participation in ensuring security. Russian influence activities, sabotage and cyberattacks can simultaneously affect public order, digital services, critical infrastructure and public trust in the state. Resilience therefore cannot be assessed solely on the basis of one institution's capabilities or an individual technical safeguard. The central question is how threat prevention and detection, responses to attacks and the continued functioning of society relate to one another. Estonia's 2026 National Security Concept treats Russian hybrid operations as a persistent instrument of pressure whose objectives include undermining social cohesion and trust.[1]

Estonia's strength lies in combining different protective measures. An informed population helps identify threats, effective institutions enable responses, and resilient services limit the societal impact of attacks.

The purpose of this overview is to analyse the main institutional and societal components of Estonia's preparedness. It draws on two interconnected approaches: coordination across government, or the whole-of-government principle, and the involvement of society as a whole, or the whole-of-society principle. The former concerns the division of responsibilities and cooperation among institutions; the latter concerns the contributions of individuals, communities, businesses and volunteers. Estonia's geographical position and historical experience provide additional context for this approach.

The overview focuses on the following interconnected areas: education and psychological defence, the public exposure of threats, the continuity of essential services, border protection and internal security, cybersecurity, and the involvement of volunteers. Military training is discussed where it relates to societal cooperation and the development of skills; this overview is not an assessment of military defence capability. The analysis draws on publicly available strategic documents, descriptions of institutional responsibilities, training programmes and documented cases. It therefore primarily describes the organisation of preparedness and the conditions for its effective functioning, rather than classified capabilities or the measured effectiveness of every measure.

The central argument is that Estonia's strength lies in combining different protective measures. An informed population helps identify threats, effective institutions enable responses, and resilient services limit the societal impact of attacks.

Psychological Defence and Educational Preparedness

One form of societal preparedness is conscription. Its primary purpose is to train military reserve units, but shared training also creates opportunities for cooperation among people from different social, educational and linguistic backgrounds. Conscription does not depend on political views or a family's financial circumstances. From the perspective of social cohesion, what matters is performing a shared task that requires consideration for others.

[1] Government Office, "National Security Concept of Estonia. 3. Security Environment," 2026, https://riigikantselei.ee/jpa/julgeolekukeskkond

Men remain liable for military service until the age of 60 and, while in the reserve, participate in reservist training exercises as required. Women may voluntarily assume the obligation to perform military service.[2] Given Estonia's demographic realities and the growing needs of the Defence Forces in the current geopolitical situation, making conscription compulsory for women in the near future is probably inevitable.

The education system's role is to develop the knowledge and skills needed to evaluate information critically. Media literacy encompasses analysing messages, images and claims presented through different channels, understanding their context, and creating content responsibly. The Ministry of Education and Research explicitly links the development of media literacy to safeguarding democracy and security. It is therefore reasonable to regard it as part of long-term resilience.[3]

Educational preparedness also extends to higher education. The University of Tartu's master's programme in Disinformation and Societal Resilience focuses on understanding information manipulation and applying theoretical knowledge to problems faced by organisations and communities. General education and specialised master's studies fulfil different roles: the former develops broader awareness, while the latter trains specialists with in-depth knowledge. Both support people's ability to navigate the information environment.[4]

National defence education in upper secondary schools provides knowledge needed in a crisis. Its theoretical course has been compulsory in all upper secondary schools since autumn 2023. Voluntary practical training complements theoretical instruction. The course's value extends beyond introducing military defence: it helps students understand civic responsibility and acquire skills applicable to everyday life. Practical knowledge can make abstract threats easier to understand.[5]

The Higher National Defence Courses play an important role in preparing adults and decision-makers. They have been held in their current form since 1999 and are organised by the International Centre for Defence and Security. Their target audience includes politicians, officials, military personnel, business leaders, journalists, figures from education and culture, and civil society representatives. The aim is to introduce Estonia's security, foreign and defence policies and enhance cooperation. They are therefore not merely professional training for officials, but a learning environment bringing together different sections of society.[6]

The analytical value of the courses' design lies in combining knowledge with professional connections. Understanding the organisation of national defence helps participants recognise how their own field relates to other actors. Joint discussions allow officials to learn about the perspectives of businesses and communities, while enabling the latter to better understand the responsibilities of state institutions. Such contact does not replace formal management arrangements, but it can support cooperation when a problem extends beyond one organisation's remit. Both the course content and the opportunity to develop a shared understanding of national defence are therefore important.

---

2 Estonian Defence Forces, "How Long Does Conscript Service Last?," https://mil.ee/ajateenistus/kui-kaua-kestab-ajateenistus/; Defence Resources Agency, "Conscript Service," https://kra.ee/ajateenistus/

3 Ministry of Education and Research, "Media Literacy," https://www.hm.ee/meediapadevus

4 University of Tartu, "Disinformation and Societal Resilience," https://ut.ee/et/oppekavad/desinformatsioon-ja-uhiskondlik-toimepidevus

5 Ministry of Defence, "National Defence Education," https://www.kaitseministeerium.ee/kaitsetahe-toetused-ja-haridusprogrammid/riigikaitseline-jarelkasv-ja-haridus/riigikaitseopetus

6 Ministry of Defence, "Higher National Defence Courses," https://www.kaitseministeerium.ee/kaitsetahe-toetused-ja-haridusprogrammid/kaitsetahte-arendamine/korgemad-riigikaitsekursused

Alongside the Estonian National Defence Courses, national defence courses are organised for business leaders. Delivered jointly by the Ministry of Defence and the International Centre for Defence and Security, this training introduces the functioning of the reserve-based military, Defence Forces training, and employers' role in national defence. For business leaders, it helps explain employees' participation in reservist training exercises and the value of the skills acquired during training. It also highlights the interdependence of the private sector and the state: national defence requires employers' support, while businesses need a secure operating environment. Cooperation requires both sides to understand each other's responsibilities and constraints.[7]

A student, a business leader and a local government representative have different responsibilities, so offering everyone only the same general description of threats is insufficient.

The Advanced Cybersecurity and Digital State Course connects cyber issues with management decisions. The description of the 2026 course, organised by the International Centre for Defence and Security and the Ministry of Justice and Digital Affairs, emphasises the architecture and dependencies of the digital state and the cybersecurity threat landscape. Its target audience includes public- and private-sector leaders, journalists and policymakers. The course aims to help participants understand how a secure digital society functions, rather than turn all participants into technical experts. Awareness at management level is necessary because mitigating technical risks also requires organisational decisions.[8]

The Advanced Civil Protection Course, led by the Rescue Board, focuses on people's crisis preparedness, the division of responsibilities between central and local government, and the tasks of the health and social care sectors. The courses have been held since 2022, with participants including central and local government leaders, experts and journalists. The approach centres on the relationship between individual preparedness and institutional capacity. When participants understand what assistance they provide and what assistance they expect from others, more realistic crisis preparedness becomes possible.[9]

Psychological defence courses focus on information influence activities and cooperation among partners from different linguistic and cultural backgrounds. The course is intended to develop connections among communications specialists, journalists, opinion leaders and local networks. Central to this approach is the ability to reach people through partners familiar with the local environment. The existence of an official message alone does not ensure that it is understood or trusted. Building contacts and a shared information environment are therefore practical elements of psychological defence.[10]

The different forms of educational preparedness share the understanding that security knowledge must reach people's own fields of activity. A student, a business leader and a local government representative have different responsibilities, so offering everyone only the same general description of threats is insufficient. Shared principles need to be linked to specific responsibilities. Courses and educational activities can help people understand when to act independently, when to share information and when to seek assistance from the competent authority. This connection helps translate awareness into practical preparedness.

7 Ministry of Defence, "National Defence Course for Business Leaders," https://www.kaitseministeerium.ee/kaitsetahe-toetused-ja-haridusprogrammid/kaitsetahte-arendamine/ettevotjatele-suunatud

8 International Centre for Defence and Security, "Invitation to the 12th Advanced Digital State and Cyber Defence Course," 2026, https://dokumendiregistrid.karlerss.com/dokumendid/924623/kutse-osa-lemiseks-xii-korgematel-digiriigi-ja-kuberkaitse-kursustel

9 Rescue Board, "The First Advanced Civil Protection Course of the Year, and the Sixth Overall, Was Held," April 8, 2024, https://www.rescue.ee/et/uudised/toimus-selle-aasta-esimene-jaerjekorras-juba-kuues-korgem-elanikkonnakaitse-kursus-kekk-2287

10 Ministry of Culture, "Letter," section "Psychological Defence Course in Ida-Viru County," https://dokumendiregistrid.karlerss.com/dokumendid/742007/kiri

Nor does preparation end with the completion of a single course. Changes in the threat landscape, technology and people's responsibilities mean that previously acquired knowledge must be updated. The diversity of the courses discussed allows this to be approached from different perspectives, connecting national defence, the digital state and civil protection. Their combined value lies not in providing identical training to all participants, but in developing a shared understanding of responsibility. This is particularly necessary when people with different professional backgrounds must address the consequences of the same crisis.

Public Exposure of Threats and Societal Continuity

People who recognise signs of influence activities or recruitment can adjust their behaviour and, where necessary, notify the competent authority.

The public discussion of security threats has an important place in Estonia's approach. The Estonian Internal Security Service published its first annual review in 1998. The review aims to inform the public about security risks and develop an understanding of the service's activities. This allows descriptions of specific cases to be connected to the broader threat landscape. Public disclosure does not, however, amount to complete transparency: the protection of individuals and operational requirements limit the information that can be released. The annual review should therefore be treated as a selective public account, rather than a comprehensive register of all known threats.[11]

Publicly exposing threats can both support prevention and build trust. People who recognise signs of influence activities or recruitment can adjust their behaviour and, where necessary, notify the competent authority. Public discussion of cases also demonstrates that the state is investigating them. A possible deterrent effect may arise from the knowledge that suspicious activities will be detected and exposed.

Journalism and voluntary initiatives complement the work of state institutions. Propastop is a blog run by Defence League volunteers that seeks to expose anti-Estonian propaganda and information manipulation. Its work includes checking claims against facts, explaining context and identifying actors with an interest in exerting influence. This gives the public additional opportunities to evaluate messages circulating in the information environment. The value of such activity depends on verifiable evidence and a clear distinction between facts and interpretations.[12]

Alongside public disclosure, the state must limit the practical consequences of attacks. The arrangements for ensuring the continuity of essential services require service providers to assess their risks and prepare for crises. Risk assessments must connect threats to the activities and resources needed to deliver a service. Their purpose is to identify which disruptions to activities threaten service continuity and which measures are needed to prevent or mitigate an interruption. Plans demonstrate their value above all when the responsibilities and solutions they describe correspond to the organisation's actual capabilities.[13]

11 Estonian Internal Security Service, "The History and Purpose of the Annual Review," https://kapo.ee/et/aastaraamatud/.

12 Propastop, "What Is Propastop?," https://www.propastop.org/about/

13 Government Office, "KORKS Handbook. 1.1.7. Risk Assessment by an Essential Service Provider," https://riigikantselei.ee/korks-kasiraamat/117-elutahtsa-teenuse-osutaja-riskianaluus

Reducing risks arising from people is also part of ensuring continuity. According to the Government Office's handbook, an essential service provider must identify in its risk assessment the tasks for which background checks are necessary. The identities and criminal records of those performing these tasks are then checked to the extent prescribed by law. This is not an unrestricted background investigation of all employees. The distinction matters because security measures must be linked to a specific task and a legal basis. Supply chains, physical security and personnel reliability form an integrated whole together with technical measures.[14]

To manage digital risks, the Information System Authority has developed the Estonian Information Security Standard, E-ITS. The standard supports information security management tailored to individual organisations and provides access to a catalogue of security measures. It enables protection requirements to be linked to an organisation's services, work processes and technical solutions. The existence of a standard does not automatically ensure security: measures must be implemented, their effectiveness checked, and adjustments made as circumstances change. Developing staff awareness forms part of these arrangements and must reflect the organisation's risks and employees' responsibilities.[15]

The existence of a standard does not automatically ensure security: measures must be implemented, their effectiveness checked, and adjustments made as circumstances change.

Estonia's National Security Concept also sets an objective for security of supply as part of societal crisis resilience. Stockpiles and other arrangements must enable society as a whole to cope for at least 30 days in a crisis or war, until the necessary connections are restored. This is a strategic objective encompassing the state, businesses, local governments and residents.[16]

Exercises make it possible to test whether different actors' plans fit together. The main week of the large-scale ILVES 2026 exercise took place on 8–12 June and, according to the Government Office's summary, involved approximately 4,000 people from more than 150 organisations. Participants included the country's highest leadership, local governments, businesses and civic organisations. Activities practised included management, public information, maintaining public order, evacuation and the operation of essential services. The range of participants reflects the principle of comprehensive national defence: resolving a crisis requires cooperation beyond the conventional security institutions.[17]

The scale of an exercise indicates the extent to which cooperation is practised, but the number of participants does not in itself demonstrate the adequacy of all capabilities. The analytical value of exercises lies in the opportunity to compare planned activities with actual decision-making and information exchange. Developing preparedness requires guidance given to residents and institutions to be reinforced through practical exercises. The same principle means that shortcomings identified during exercises require follow-up action. Otherwise, participation remains a one-off experience rather than becoming part of an organisation's lasting preparedness.

14 Government Office, "KORKS Handbook. 3.6.1. Essential Service Provider," https://riigikantselei.ee/korks-kasiraamat/361-elutahtsa-teenuse-osutaja

15 Information System Authority, "Estonian Information Security Standard (E-ITS)," https://www.ria.ee/kuberturvalisus/riigi-infoturbe-meetmete-haldus/eesti-infoturbestandard-e-its

16 Government Office, "National Security Concept of Estonia. 4.2. Economic Security and Essential Services," 2026, https://riigikantselei.ee/jpa/majandusjulgeolek-ja-elutahtsad-teenused

17 Government Office, "ILVES 2026 Became the Largest Crisis Exercise in Estonia's History," June 12, 2026, https://riigikantselei.ee/uudised/ilves-2026-kasvas-eesti-ajaloo-suurimaks-kriisioppuseks; Government Office, "Large-Scale Exercise ILVES 2026," June 5, 2026, https://riigikantselei.ee/ilves

The focus on continuity also connects infrastructure protection with public trust. When a service is interrupted, people need information about both what has happened and how to respond. Technical recovery and crisis communication therefore cannot be treated as separate activities. At the same time, explanations do not replace service restoration, nor do stockpiles replace effective distribution. Under the approach discussed here, each actor must take account of others' capabilities and dependencies, so that one organisation's plan does not assume assistance that another is unprepared to provide.

Border Protection and Internal Security

As a country on the external borders of the European Union and NATO, Estonia connects border protection with internal security and international cooperation. The merged Police and Border Guard Board began operating on 1 January 2010. The unified agency model allows border crossings to be considered alongside issues involving documents, the right to remain in the country and possible criminal activity. This matters in the context of hybrid threats because a single incident can have several dimensions at once. Organisational integration creates the conditions for cooperation.[18]

Following the start of Russia's full-scale aggression against Ukraine, Estonia has supplemented border checks with entry restrictions. Applying these restrictions requires checking the purpose of travel and the right of entry in addition to travel documents. Border protection therefore encompasses physical surveillance as well as administrative and legal decisions.[19]

The operation of border crossing points has also been restricted, including through reduced overnight opening hours. These measures complement border surveillance and customs controls. Estonia also supports neighbouring countries by deploying ESTPOL teams to the Latvia–Belarus border as part of long-term cooperation. Regional cooperation is relevant because pressure at the external border can spread through movement between countries. This creates a need to connect developments at the border with situational awareness inside the country.[20]

A strength of the internal security system is its ability to connect threat detection, prevention, investigation and crisis response. Agencies within the Ministry of the Interior's area of responsibility play a central role, but cooperation also involves the prosecutor's office, cybersecurity authorities, local governments and businesses. Nationwide arrangements create opportunities for common working standards and the pooling of resources. This has practical value for a small state, since it is not possible to maintain every specialist capability separately in every region. At the same time, sufficient personnel, replacements and equipment remain decisive in a prolonged crisis.

---

18 Government of the Republic of Estonia, "Annotated Agenda for the Government Meeting of 18 June 2009," agenda item 14, June 18, 2009, https://valitsus.ee/uudised/valitsuse-18062009-istungi-kommenteeritud-paevakord

19 Government of the Republic of Estonia, "Temporary Restrictions on Crossing the State Border by Citizens of the Russian Federation," Order No. 247, version effective January 25, 2026, September 8, 2022, https://www.riigiteataja.ee/akt/323012026006

20 Ministry of Foreign Affairs, "Russia," May 15, 2026, https://reisitargalt.vm.ee/sihtkoht/venemaa/; Ministry of the Interior, "Estonia Extends Its Border Guard Mission on the Latvia–Belarus Border," September 22, 2026, https://www.siseministeerium.ee/uudised/eesti-pikendab-piirivalvemissiooni-lati-valgevene-piiril

An important feature of the Estonian Internal Security Service is its combination of counterintelligence and criminal investigation powers. Within its remit, the service can examine the activities of a foreign intelligence service together with recruitment, intermediaries and specific crimes. Its public description of its responsibilities emphasises its functions as both a security service and an investigative authority. This arrangement can make it easier to connect information, but it does not remove evidentiary requirements or the prosecutor's role. The institutional advantage must therefore be understood as an opportunity whose actual use depends on the circumstances of each case.[21]

This relationship is illustrated by the damage to the cars of the interior minister and a journalist in December 2023. According to a statement issued by the prosecutor's office on 5 December 2024, Allan Hantsom was convicted of organising the attack at the GRU's request and under its direction. The investigation uncovered a chain of intermediaries and distinguished organisers who knew the crime's true purpose from perpetrators who did not. The case demonstrates why an apparent property crime may, where appropriate, also need to be investigated in the context of a foreign state's influence activities. It also underlines the importance of evidence that can be tested in court.[22]

Cybersecurity

Cybersecurity complements internal security because damage to digital systems can affect government operations, service delivery and public trust. Estonia's arrangements can be analysed as several mutually reinforcing levels: user and organisational security, the protection of data exchange, national monitoring and supervision, law enforcement, and voluntary and military cyber defence. This distinction helps clarify responsibilities, but it does not mean that these levels operate separately. A vulnerability or incident detected in one organisation may require cooperation among several actors.

The first level of protection concerns devices, accounts and everyday work processes. Secure authentication, software updates, restrictions on access rights, network segmentation and backups reduce the opportunities available to an attacker. An organisation's management must know which services and data are critical and who is responsible for protecting them. Staff awareness supports technical measures but does not replace them. The organisation must also consider how work will continue during an interruption and the order in which normal operations will be restored.[23]

The digital state is supported by the X-tee data exchange layer. According to the Information System Authority's description, it uses authentication, access control, logging, and encrypted and digitally signed data traffic. X-tee allows different information systems to exchange information securely without consolidating all data in a single central database. Its value lies in protected and traceable data exchange. However, joining X-tee does not automatically make

21 Estonian Internal Security Service, "The History and Purpose of the Annual Review."

22 Prosecutor's Office, "Allan Hantsom Organised the Vandalism of the Interior Minister's and a Journalist's Cars at the GRU's Request," December 5, 2024, https://www.prokuratuur.ee/uudised/siseministri-ja-ajakirjaniku-auto-lohkumise-organiseeris-gru-ulesandel-allan-hantsom

23 Information System Authority, "Estonian Information Security Standard (E-ITS)."

an organisation's own applications or user accounts secure. Participants remain responsible for protecting their own systems even when using a shared data exchange environment.[24]

At the national level, the Information System Authority combines advice to organisations with statutory supervision. Supervision checks the implementation of security measures, and compliance orders can be issued when shortcomings are identified. Its purpose is to make compliance verifiable and direct organisations to remedy weaknesses. The system's strength lies not only in setting requirements but also in being able to monitor remedial action. Service providers nevertheless remain responsible for their own systems: supervision does not take over an organisation's day-to-day information security management.[25]

Resolving a technical incident may not address every security issue. Where necessary, perpetrators must be identified, evidence collected, and the purpose of the attack and any possible link to a foreign state established.

CERT-EE, part of the Information System Authority, serves as the national cyber incident response team. It monitors Estonian cyberspace around the clock, detects incidents, helps investigate their causes and advises on their resolution. A national perspective makes it possible to compare events observed in different organisations and share threat information. An apparently isolated incident can thus, where appropriate, be linked to a broader pattern of attacks. CERT-EE's role is primarily to support situational awareness and technical response, making prompt cooperation with the affected organisation essential.[26]

Resolving a technical incident may not address every security issue. Where necessary, perpetrators must be identified, evidence collected, and the purpose of the attack and any possible link to a foreign state established. This is where cybersecurity connects with law enforcement and counterintelligence. From a security perspective, it is important, where possible, to move beyond the individual damage to identify those responsible for organising it and their methods. Technical attribution and establishing proof in criminal proceedings are not, however, equivalent activities. Responding to a cyberattack therefore also requires clear responsibilities and institutional cooperation.

Additional expertise is provided by the Defence League's Cyber Defence Unit, which brings together volunteer specialists from the public and private sectors. The unit operates nationwide, and members living abroad can also participate in its activities. These arrangements make it possible to draw on knowledge that is not all concentrated within the state's permanent workforce. Voluntary participation is nevertheless an effective capability only when tasks, training and leadership arrangements have been prepared. Professional competence provides a basis for contributing, but cooperation during a crisis also requires joint practice.[27]

The Defence Forces' Cyber Command organises cyber defence within the military sphere of responsibility. Its Cyber and Information Operations Centre is responsible for protecting information systems and data, conducting operations, and training reserve units. For the purposes of this overview, the distinction between areas of responsibility is important: securing civilian services and protecting military command and control are related but different tasks. Cooperation must help prevent gaps between them while preserving each actor's responsibilities. The existence of military cyber capabilities does not relieve civilian institutions or businesses of the duty to protect their own systems.[28]

[24] Information System Authority, "X-tee Data Exchange Layer," https://www.ria.ee/riigi-infosusteem/andmevahetuse-platvormid/andmevahetuskiht-x-tee

[25] Information System Authority, "Administrative and State Supervision," https://ria.ee/kuberturvalisus/jarelevalve

[26] Information System Authority, "Cyber Incident Response CERT-EE," https://www.ria.ee/kuberturvalisus/kuberintsidentide-kasitlemine-cert-ee

[27] Defence League Cyber Defence Unit, "Activities of the Defence League's Cyber Defence Unit," https://kuberkaitseliit.ee/tegevus/

[28] Estonian Defence Forces, "Cyber and Information Operations Centre," https://mil.ee/uksused/kubervaejuhatus/kuber-ja-infooperatsioonide-keskus/

Cybersecurity also encompasses recovery after a successful attack. Verified backups, rehearsed recovery procedures and alternative ways of working help reduce the duration of an interruption. Estonia's data embassy in Luxembourg supports digital continuity by enabling important data and services to be backed up and, where necessary, operated outside Estonian territory. This does not mean that all government services automatically continue uninterrupted abroad. The data embassy is part of a recovery capability whose use depends on the database owner's preparations and the effectiveness of recovery processes.[29]

The interaction between the different levels of cybersecurity demonstrates why preparedness cannot be reduced to a single technological solution. An organisation must detect an incident, communicate the information to the appropriate recipient and take responsibility for recovery. National monitoring and supervision support these activities but do not remove the organisation's own need to make decisions. Involving a volunteer expert also requires arrangements for their tasks and access rights. Professional expertise and the ability to operate within agreed responsibilities are therefore equally important in cybersecurity.

The interaction between the different levels of cybersecurity demonstrates why preparedness cannot be reduced to a single technological solution.

Reserves and Volunteers

For a small state's crisis resilience, the ability to involve people outside institutions' permanent staff is important. The volunteers described above combine specialist expertise, knowledge of the local environment and a willingness to contribute. Personnel reserves cannot, however, be assessed solely by the number of members or registered individuals. It is necessary to know who has been trained, what task they have been assigned and whether they can participate during a crisis. It is particularly important to avoid a situation in which an employer and several voluntary organisations all count on the same person simultaneously.

The Defence League's contribution to communities is complemented by the Women's Voluntary Defence Organisation and youth organisations. For the purposes of this discussion, the Women's Voluntary Defence Organisation's civil protection activities are particularly relevant: teaching crisis preparedness and assisting people. Its mobile application "Be Prepared!" brings together official guidance on how to act, first aid information and tools for assessing household emergency supplies. This allows practical guidance to reach beyond the organisation's membership. Access to guidance supports preparedness.[30]

The Women's Voluntary Defence Organisation has also contributed in actual crises. Its overview of 2020 describes support to the police, the Health Board, the Emergency Response Centre and local governments, as well as assistance at hospitals. This demonstrates that a volunteer network can perform a range of supporting tasks. It should not be taken to imply unlimited capacity to replace regular personnel: assistance must match people's skills and the receiving institution's needs. Experience of participating in crises is a more meaningful indicator of preparedness than membership numbers alone, although it does not automatically guarantee the ability to cope with a different type of crisis.[31]

---

29 Ministry of Foreign Affairs, "Luxembourg," https://vm.ee/luksemburg; State IT Centre, "Data Embassy: Secure Storage for [Critically] Important Databases," https://www.rit.ee/teenused-andmesaatkond

30 Women's Voluntary Defence Organisation, "Be Prepared!," https://www.naiskodukaitse.ee/OLE_VALMIS_3680.

31 Women's Voluntary Defence Organisation, "The 2020 Crisis Increased Activity among Members of the Women's Voluntary Defence Organisation," https://www.naiskodukaitse.ee/2020_aasta_kriis_tostis_4546

Internal security benefits from assistant police officers, volunteer rescuers, maritime rescue volunteers, volunteer explosive ordnance disposal assistants and Emergency Response Centre volunteers. According to the Ministry of the Interior's 2026 overview, Estonia has more than 3,000 volunteer rescuers, nearly 1,300 assistant police officers, around 850 maritime rescue volunteers, approximately 100 volunteer explosive ordnance disposal assistants and roughly 150 Emergency Response Centre volunteers. These groups provide additional personnel with different training and tasks. The figures cannot, however, be added together to form a single reserve deployable simultaneously, because memberships may overlap and individuals' actual availability varies.[32]

The development of the internal security crisis reserve aims to link the contributions of volunteers and former personnel to clearer crisis roles. The government approved the concept in February 2026, and the necessary draft legislation was circulated for consultation in May. The ministry explains the changes in terms of personnel needs during prolonged crises and the avoidance of overlapping roles. Existing volunteers must therefore be distinguished from the common reserve arrangements under development. The concept and draft legislation describe the intended arrangements, but they do not establish the final size of the entire reserve or its full operational readiness.[33]

When involving volunteers, a distinction must be made between willingness to help and the ability to participate over an extended period.

When involving volunteers, a distinction must be made between willingness to help and the ability to participate over an extended period. A person may be trained but also committed to their regular job, family or another crisis role. The organisation of a reserve therefore centres on agreeing roles in advance, rather than simply achieving the largest possible membership. The value of a volunteer's contribution increases when an institution can assign an appropriate task, provide guidance, and allow for shifts and rest. In this way, individual willingness becomes additional capacity that an organisation can actually use.

The same principle helps explain the importance of the community level. Knowledge of the local environment allows general guidance to be connected to specific people and needs, but the organisation of assistance must fit with the activities of the responsible institutions. Volunteers can complement the professional system both in practical tasks and in communicating information. They cannot, however, eliminate every shortfall in permanent personnel or equipment. In assessing Estonia's preparedness, volunteers must therefore be considered together with the management and resources supporting them, rather than as a separate, unlimited reserve.

When using public sources, it must also be recognised that institutional descriptions provide the clearest account of official responsibilities and arrangements. They do not necessarily describe all difficulties encountered in implementation. They therefore provide a sound basis for describing the forms of cooperation and capabilities that have been established, but assessing their adequacy requires additional data on actual performance. The conclusions of this overview remain at that level: they connect the measures described and identify the conditions for their use.

---

32 Ministry of the Interior, "The Ministry of the Interior Recognises Internal Security Volunteers and Their Supporters," 2026, https://siseministeerium.ee/uudised/siseministeerium-tunnustab-siseturvalisuse-vabatahtlikke-ja-nende-toetajaid

33 Ministry of the Interior, "The Government Gives the Green Light to Establish a Crisis Reserve within the Ministry of the Interior's Area of Responsibility," February 20, 2026, https://www.siseministeerium.ee/uudised/valitsus-andis-rohelise-tule-siseministeeriumi-valitsemisala-kriisireservi-loomiseks; Ministry of the Interior, "Interior Minister Taro: A Reserve Helps Ensure Internal Security during Crises," May 26, 2026, https://www.siseministeerium.ee/uudised/siseminister-taro-reserv-aitab-tagada-siseturvalisust-ka-kriisiolukorras

This delineation also helps avoid conflating different forms of preparedness. The long-term impact of education, the police response to a specific crime and the restoration of an essential service are interconnected, but they cannot be assessed using a single indicator. Societal resilience emerges from their combined effects, while those responsible for each field must separately ensure that their own tasks are fulfilled.

Conclusion

Estonia's preparedness to counter Russian hybrid threats develops through several interconnected areas of activity. Education and courses help people understand threats and build cooperative relationships. Public communication by security agencies, journalism and voluntary initiatives support the identification of influence activities. Internal security arrangements enable threat detection and criminal investigation to be connected, while the continuity of essential services and cyber defence reduce the impact of attacks on the functioning of the state and society. None of these components is independent of the others.

A central condition for Estonia's resilience is the consistent implementation and interaction of existing measures.

The examples discussed in this overview support the conclusion that the central strength of Estonia's model is its treatment of security as a shared responsibility. Courses bring together representatives of different fields, exercises connect state institutions with businesses and local governments, and volunteers enable additional skills to be mobilised. These arrangements create the conditions for action when an attacker uses several instruments of pressure at once. Their value lies in translating awareness into practical action and connecting the resolution of individual incidents to the continued functioning of society.

At the same time, a list of institutions, programmes and membership figures does not allow a definitive conclusion about the adequacy of Estonia's preparedness. A strategic objective differs from an achieved capability, participation in an exercise from verified effectiveness, and a list of volunteers from an actually available reserve. The same applies to technical solutions: secure data exchange and backups require effective organisations, competent people and rehearsed recovery procedures. These distinctions are necessary to avoid overstating preparedness and to maintain the analysis's verifiability.

A central condition for Estonia's resilience is the consistent implementation and interaction of existing measures. Clear crisis roles, the actual availability of staff and volunteers, effective information exchange, and the correction of shortcomings identified in exercises are decisive. Estonia's experience indicates that countering hybrid threats is an ongoing societal and institutional activity. Its effectiveness must be assessed by whether people and institutions can continue to fulfil their responsibilities under pressure and maintain or restore essential services.

Bibliography

Defence League Cyber Defence Unit. "Activities of the Defence League's Cyber Defence Unit." https://kuberkaitseliit.ee/tegevus/

Defence Resources Agency. "Conscript Service." https://kra.ee/ajateenistus/

Estonian Defence Forces. "Cyber and Information Operations Centre." https://mil.ee/uksused/kubervaejuhatus/kuber-ja-infooperatsioonide-keskus/

Estonian Defence Forces. "How Long Does Conscript Service Last?" https://mil.ee/ajateenistus/kui-kaua-kestab-ajateenistus/

Estonian Internal Security Service. "The History and Purpose of the Annual Review." https://kapo.ee/et/aastaraamatud/

Government of the Republic of Estonia. "Annotated Agenda for the Government Meeting of 18 June 2009." June 18, 2009. https://valitsus.ee/uudised/valitsuse-18062009-istungi-kommenteeritud-paevakord

Government of the Republic of Estonia. "Temporary Restrictions on Crossing the State Border by Citizens of the Russian Federation." September 8, 2022. Order No. 247. RT III, 10.09.2022, 2; version published in RT III, 23.01.2026, 6. https://www.riigiteataja.ee/akt/323012026006

Government Office. "ILVES 2026 Became the Largest Crisis Exercise in Estonia's History." June 12, 2026. https://riigikantselei.ee/uudised/ilves-2026-kasvas-eesti-ajaloo-suurimaks-kriisioppuseks

Government Office. "KORKS Handbook. 1.1.7. Risk Assessment by an Essential Service Provider." October 2, 2026. https://riigikantselei.ee/korks-kasiraamat/117-elutahtsa-teenuse-osutaja-riskianaluus

Government Office. "KORKS Handbook. 3.6.1. Essential Service Provider." https://riigikantselei.ee/korks-kasiraamat/361-elutahtsa-teenuse-osutaja

Government Office. "Large-Scale Exercise ILVES 2026." June 5, 2026. https://riigikantselei.ee/ilves

Government Office. "National Security Concept of Estonia. 3. Security Environment." 2026. https://riigikantselei.ee/jpa/julgeolekukeskkond

Government Office. "National Security Concept of Estonia. 4.2. Economic Security and Essential Services." 2026. https://riigikantselei.ee/jpa/majandusjulgeolek-ja-elutahtsad-teenused

Information System Authority. "Administrative and State Supervision." https://ria.ee/kuberturvalisus/jarelevalve

Information System Authority. "Cyber Incident Response CERT-EE." https://www.ria.ee/kuberturvalisus/kuberintsidentide-kasitlemine-cert-ee

Information System Authority. "Estonian Information Security Standard (E-ITS)." https://www.ria.ee/kuberturvalisus/riigi-infoturbe-meetmete-haldus/eesti-infoturbestandard-e-its

Information System Authority. "X-tee Data Exchange Layer." https://www.ria.ee/riigi-infosusteem/andmevahetuse-platvormid/andmevahetuskiht-x-tee

International Centre for Defence and Security. "Invitation to the 12th Advanced Digital State and Cyber Defence Course." 2026. https://dokumendiregistrid.karlerss.com/dokumendid/924623/kutse-osalemiseks-xii-korgematel-digiriigi-ja-kuberkaitse-kursustel

Ministry of Culture. "Letter." Accessed October 28, 2026. Section of the planning document "Psychological Defence Course in Ida-Viru County." https://dokumendiregistrid.karlerss.com/dokumendid/742007/kiri

Ministry of Defence. "Estonian National Defence Courses." https://www.kaitseministeerium.ee/kaitsetahe-toetused-ja-haridusprogrammid/kaitsetahte-arendamine/korgemad-riigikaitsekursused

Ministry of Defence. "National Defence Course for Business Leaders." https://www.kaitseministeerium.ee/kaitsetahe-toetused-ja-haridusprogrammid/kaitsetahte-arendamine/ettevotjatele-suunatud

Ministry of Defence. "National Defence Education." https://www.kaitseministeerium.ee/kaitsetahe-toetused-ja-haridusprogrammid/riigikaitseline-jarelkasv-ja-haridus/riigikaitseopetus

Ministry of Education and Research. "Media Literacy." https://www.hm.ee/meediapadevus

Ministry of Foreign Affairs. "Luxembourg." https://vm.ee/luksemburg

Ministry of Foreign Affairs. "Russia." May 15, 2026. https://reisitargalt.vm.ee/sihtkoht/venemaa/

Ministry of the Interior. "Estonia Extends Its Border Guard Mission on the Latvia–Belarus Border." September 22, 2026. https://www.siseministeerium.ee/uudised/eesti-pikendab-piirivalvemissiooni-lati-valgevene-piiril

Ministry of the Interior. "The Government Gives the Green Light to Establish a Crisis Reserve within the Ministry of the Interior's Area of Responsibility." February 20, 2026. https://www.siseministeerium.ee/uudised/valitsus-andis-rohelise-tule-siseministeeriumi-valitsemisala-kriisireservi-loomiseks

Ministry of the Interior. "Interior Minister Taro: A Reserve Helps Ensure Internal Security during Crises." May 26, 2026. https://www.siseministeerium.ee/uudised/siseminister-taro-reserv-aitab-tagada-siseturvalisust-ka-kriisiolukorras

Ministry of the Interior. "The Ministry of the Interior Recognises Internal Security Volunteers and Their Supporters." 2026. https://siseministeerium.ee/uudised/siseministeerium-tunnustab-siseturvalisuse-vabatahtlikke-ja-nende-toetajaid

Propastop. "What Is Propastop?" https://www.propastop.org/about/

Prosecutor's Office. "Allan Hantsom Organised the Vandalism of the Interior Minister's and a Journalist's Cars at the GRU's Request." December 5, 2024. https://www.prokuratuur.ee/uudised/siseministri-ja-ajakirjaniku-auto-lohkumise-organiseeris-gru-ulesandel-allan-hantsom

Rescue Board. "The First Advanced Civil Protection Course of the Year, and the Sixth Overall, Was Held." April 8, 2024. https://www.rescue.ee/et/uudised/toimus-selle-aasta-esimene-jaerjekorras-juba-kuues-korgem-elanikkonnakaitse-kursus-kekk-2287

State IT Centre. "Data Embassy: Secure Storage for [Critically] Important Databases." https://www.rit.ee/teenused-andmesaatkond

University of Tartu. "Disinformation and Societal Resilience." https://ut.ee/et/oppekavad/desinformatsioon-ja-uhiskondlik-toimepidevus

Women's Voluntary Defence Organisation. "Be Prepared!" https://www.naiskodukaitse.ee/OLE_VALMIS_3680

Women's Voluntary Defence Organisation. "The 2020 Crisis Increased Activity among Members of the Women's Voluntary Defence Organisation." https://www.naiskodukaitse.ee/2020_aasta_kriis_tostis_4546



The Hague Centre
for Strategic Studies

HCSS
Lange Voorhout 1
2514 EA The Hague

Follow us on social media:
@hcssnl

The Hague Centre for Strategic Studies
Email: info@hcss.nl
Website: www.hcss.nl