RAUL SAVIMAA, JAANIKA PUUSALU, EMILIA MUUGA, RIINA KERNER, GEORG-HENRI KAUP, INDREK PAADIK

COMPREHENSIVE NATIONAL DEFENCE STRATEGY IN THE FIELD OF INTERNAL SECURITY: AN OVERVIEW OF 34 COUNTRIES' NATIONAL DEFENCE MODELS

RESEARCH REPORT

**RAUL SAVIMAA, JAANIKA PUUSALU,
EMILIA MUUGA, RIINA KERNER,
GEORG-HENRI KAUP, INDREK PAADIK**

Comprehensive National Defence Strategy in the Field of Internal Security: an Overview of 34 Countries' National Defence Models

RESEARCH REPORT

VERBIS AUT RE

CONTENTS

EXECUTIVE SUMMARY

This report examines the design and implementation of comprehensive defence strategies by different countries in the field of internal security. In doing so, it supports an evidence-based approach to the further development of Estonia's national defence strategy (hereinafter, also referred to as its comprehensive defence strategy). By focusing on international practices, the report identifies effective approaches to comprehensive defence as well as additional complexities that arise for different states as a result of their specific security needs.

The comparative analysis of different states' strategic documents and implementation practices provides a basis for assessing Estonia's specific needs as a small-sized European country facing contemporary geopolitical threats and developing a comprehensive defence framework to meet those needs. In addition to supporting national military defence, internal security institutions and policies are responsible for safeguarding societal stability and resilience and preventing critical threats such as cyberattacks, the spread of disinformation and hybrid threats. Accordingly, the aim of the study is to support a comprehensive approach to Estonian national defence, which, in addition to military defence, must involve internal security, the civilian sector, private enterprises and civil society.

When assessing Estonia's national defence practices, it is vital to take into account the specifics of its security situation, including the state's geopolitical position, security threats and societal needs. Reflecting this, the report first examines the models of comprehensive defence implemented by other, similarly small-sized European countries. To ensure that the valuable lessons that can be drawn from other kinds of states are not overlooked, the sample is then expanded to include several larger, as well as non-European, states.

The report is based on an exploratory study that mapped the comprehensive defence strategies of 34 countries, including the processes for developing these strategies and the approaches applied. The sample includes Finland, Sweden, Denmark, Norway, Latvia, Lithuania, Poland and a range of other European and worldwide examples. The study draws on publicly available online sources that provide evidence on national security strategies and strategy development processes. These sources include national strategic documents, legislation, reports, analyses, press releases and academic literature. The report highlights key strategic trends in and components of border security, cybersecurity, hybrid threats, the spread of disinformation and misinformation, civil–military cooperation, crisis resilience, evidence-based planning, and international cooperation. For several countries, there was no publicly available description of the strategy development process. Nonetheless, it was still possible to identify and provide an overview of their approach to national defence and its main focus areas from the perspective of internal security.

THE INVOLVEMENT OF DIFFERENT LEVELS OF SOCIETY AND THE CLEAR DIVISION OF ROLES ARE KEY TO THE SUCCESS OF A COMPREHENSIVE NATIONAL DEFENCE STRATEGY.
PHOTOS: PEXELS.COM

The key findings of the study are as follows:

- The status of Estonia's eastern border as an external border of the European Union makes its protection strategically significant. In this context, many countries stress the need to develop infrastructure and effective surveillance systems to counter irregular migration and other hybrid threats.

- In digitally advanced countries such as Denmark and Norway, ensuring cyber-security is a priority. Cooperation between the public and private sectors, as well as the use of artificial intelligence, is essential for protecting critical infrastructure.

- Several countries, including Lithuania and Poland, prioritise strengthening societal resilience against disinformation and hybrid threats. This is achieved through strategic communication and by raising public awareness.

- The experiences of Denmark and Norway show that the involvement of all societal groups is essential to crisis preparation and response. Civil–military cooperation should involve state institutions, the private sector and volunteer organisations.

- In various countries, crisis preparedness training, engaging local authorities and developing innovative solutions in cooperation with research institutions and the private sector have proven effective components of comprehensive defence strategies. For example, Sweden and Norway have long invested in evidence-based approaches, including planning and international cooperation, to ensure that their security policies are sustainable. Scenario analysis and risk assessment are also important as they are necessary to best understand future trends and their potential impacts.

The recommendations of the report take into account the specificities of Estonia's geopolitical locale and build on international good practice. These recommendations are intended to support the development of Estonia's internal security capabilities and enable the Ministry of the Interior and its agencies to fulfil their comprehensive defence responsibilities, including in wartime. The recommendations are as follows:

- **Strengthening border security:** Develop technologies and increase the Border Guard's readiness for countering hybrid threats, including by involving reserve personnel.

- **Protection of critical infrastructure:** Establish a cybersecurity centre based on public–private cooperation to strengthen resilience to digital threats.

- **Mechanisms for evidence-based planning:** Work with research institutions to develop data analysis and cooperation models that support evidence-based input into internal security strategies.

- **Public engagement and involvement:** Organise crisis-preparedness training for the general public and introduce crisis-management subjects into school curricula.

- **Scenario-based strategy:** Apply scenario analysis to take account of dynamic security threats and identify flexible solutions.

The report concludes that the success of a comprehensive defence strategy depends on having a holistic and synergistic approach that involves all levels of society. The lessons from international practice offer Estonia an opportunity to develop an effective and resilient national defence system capable of adapting to current and future security challenges.

INTRODUCTION

This research report provides an overview of how different countries approach national defence, including comprehensive defence. It focuses on the foundations and principles for developing a comprehensive defence strategy, particularly in the context of internal security. The concept of comprehensive national defence (hereinafter, also referred to as comprehensive defence) has a long tradition. However, as the diversification of modern threats forces states to address increasingly multi-dimensional security risks, it has become central to international debate and security practices. In contrast to the widely used military defence model, comprehensive defence encompasses both civilian and military elements and depends on the involvement of state institutions, private enterprises and civil society. The aim of the study described here was to identify principles for developing a comprehensive defence strategy in the context of internal security based on the approaches taken by different states. Based on these principles, as well as the country's specific needs, the report provides an evidence-based perspective on the development of a comprehensive defence framework for Estonia. The report focuses primarily on internal security, which has received comparatively less attention in the literature than the military and external security components of national defence.

Estonia's current national defence strategy is based on the comprehensive national defence concept (translated in Estonian as "*lai riigikaitse käsitlus*"), meaning that it involves all state agencies and society as a whole, not only military defence (Ministry of Defence, 2024). In comprehensive defence, the role of internal security is not only to support military defence functions but also to support and maintain societal stability and resilience. This includes addressing both routine and critical threats, as well as border security and related aspects of internal security.

The report highlights how international practice can offer Estonia, a small European country, important lessons for developing internal security capabilities in the context of comprehensive national defence tasks.

In 2023, the Riigikogu (Estonia's national parliament) approved the most recent version of the *National Security Concept of Estonia*. This document recommends that Estonia take a comprehensive approach to national defence that accounts for all trends and factors affecting national security. Consequently, the state has subsequently implemented a security policy that takes into account society as a whole and the state as a whole (Government of the Republic of Estonia, 2023, p. 2).

Estonia's geopolitical position on the eastern border of the European Union and in proximity to Russia is a significant factor in determining the direction of its security strategy. In addition, Estonia's security is also affected by global challenges such as hybrid threats, cyberattacks, the spread of disinformation across media channels and economic dependence on international supply chains. Areas of internal security that require special attention in the context of comprehensive defence include the following.

- **Border security:** Estonia's eastern border is also the external border of the European Union. Therefore, the security of that border must be a strategic priority.

- **Domestic security:** This requires the protection of Estonia's constitutional order, including against domestic threats such as terrorism, extremism and societal polarisation.

- **Public order and community engagement:** This refers to ensuring everyday societal stability and safety, including the involvement of volunteers and communities and safeguarding all residents.

- **Economic, technological and resource security:** This encompasses cybersecurity, the protection of critical infrastructure, ensuring the continuity of essential services, the availability of food and energy, access to health and social services, the stability of international supply chains and economic networks, and societal resilience, including countering related threats such as the spread of disinformation in media channels.

- **Cooperation between civilian and military organisations:** This includes mutual cooperation in peacetime and crisis situations. Such cooperation includes both situations where civilian organisations work with the military in national defence contexts and situations where the Defence Forces support society during major crises with resources, equipment and specialists. This concept is broader than classical civil–military cooperation (CIMIC), which, from the perspective of military organisations, focuses primarily on cooperation aimed at achieving military-strategic objectives in peacetime, during crises and during conflicts.

- **Civil protection:** This encompasses the state's preparedness to ensure the protection and safety of the population during major extraordinary events, including natural disasters, large-scale accidents, armed conflicts, hybrid attacks and other similar incidents.

The report assesses comprehensive defence strategies and practices across a diverse range of states, including the Nordic and Baltic countries, North America and the Asia–Pacific region. The report highlights important lessons that Estonia can take from international practice with regard to the development of its internal security capabilities in the context of comprehensive national defence tasks. The exploratory study of different states' security strategies and their implementation practices provides an evidence-based foundation for further comparative study and input relevant to the assessment of Estonia's needs and the development of its comprehensive defence framework. The report pays particular attention to international practices for increasing population-wide crisis preparedness, strengthening cybersecurity and promoting cooperation at the local level, all of which could be adapted to the Estonian context.

> The report highlights important lessons that Estonia can take from international practice with regard to the development of its internal security capabilities in the context of comprehensive national defence tasks. The exploratory study of different states' security strategies and their implementation practices provides an evidence-based foundation for further comparative study and input relevant to the assessment of Estonia's needs and the development of its comprehensive defence framework.

The guarantors of national security for small states are usually based on alliances with major powers and membership in international organisations (Thorhallsson & Wivel, 2006). One approach to analysing Estonia's comprehensive defence needs would have been to base that analysis in "small state theory" and compare Estonia only with other small states – i.e. states in which security and defence processes are similarly constrained by limited administrative capacity and scarce resources, yet,

where those processes can operate more quickly as lower levels of bureaucracy allow comparatively direct cross-sectoral communication (Randma-Liiv & Sarapuu, 2019). Indeed, Wrange *et al.* (2024) consider comprehensive defence to be a phenomenon typically employed by (but still not limited to) small states. However, since the aim was to identify best practices that might inform Estonia's national defence strategy, and these may not be limited to those implemented in small states, this study took a diverse, global sample of states. This provided a broader basis for analysis grounded in the comparison of not only the defence approaches of states within the European security space but also those of other states whose sovereignty, security and internal stability are threatened by a major or neighbouring power, a terrorist or criminal organisation, internal political tensions, or adverse environmental conditions and resource conflicts caused by climate change.

The concept of national defence based on joint and mutually supporting contributions across different sectors has been described in various terms, both internationally and in the domestic context. In Estonian, *lai riigikaitse käsitlus*, *lai riigikaitse* and *laiapindne riigikaitse* are all used. English equivalents include *comprehensive defence*, *comprehensive national defence* and *whole-of-society defence*, all of which can be traced back to the concept of *total defence.*

Total defence refers to an approach to national security aimed at increasing the resources to deter potential adversaries and successfully resist aggressive actions by involving society as a whole. This approach requires both military and civil defence preparations as well as institutionalised/organised cooperation among government ministries, civil society organisations, the private sector and the general public. The direct participation of civil society distinguishes total defence from conventional military deterrence and defence practices.

The concepts of societal resilience and territorial defence are frequently used in conjunction with total defence in international strategy and policy documents (Wither, 2020, p. 62). Resilience refers to a society's capacity to withstand and recover from shocks and stress quickly and effectively. This encompasses civilian, economic, commercial, security and law enforcement factors. Territorial defence refers to the military dimension of total defence. It is typically characterised as a defensive military posture aimed at responding to provocation through deterrence. The measures used for this purpose can include extensive mobilisation through conscription, preparations for both conventional and unconventional warfare, large-scale civil defence preparation, and readiness for active and passive resistance in the event of occupation (Wither, 2020, p. 62)

The concept of total defence is not new – during the Cold War, for example, the national defence policies of Switzerland, Finland, Sweden and Yugoslavia all mentioned the term (independently of each other). It is also not specific to Europe; for example, Israel and Singapore also follow total defence policies (Wither, 2020, p. 62). However, terminological similarities do not imply that national defence strategies are identical, nor do terminological differences necessarily indicate significant divergence. With that in mind, the following analysis considers both terminological and substantive differences between the various states' defence strategies.

METHODOLOGY

The study described in this report employed the exploratory study method, whereby the aim of an exploratory study is to map, describe and provide a foundational analysis of a phenomenon that has not yet been examined in detail (Swedberg, 2020) and, relatedly,

could not be fully explained by an approach grounded purely in existing theory (Stebbins, 2001).

To assess how different states have used the concept of comprehensive defence in their national defence strategies, a search for strategy documents and explanatory materials referring to or defining comprehensive defence was conducted on Google Search and Microsoft Bing. The search used the following English keywords and phrases: *total defence, comprehensive defence, comprehensive national defence, whole-of-society defence, national defence strategy, national defence planning strategy, internal security strategy, internal security and national defence, strategy development process for national security and internal security*, and *state security process*.

The main part of the study was an analysis of publicly available online sources. This sample consisted of texts that explain national security strategies and strategy development processes, including national strategic documents, legislation, reports, analyses and press releases, as well as relevant academic literature. Document collection took place between September and December 2024. Reflecting the use of solely English keywords, the analysis was primarily based on English-language materials. The total number of documents included in the study was around 120, most of them strategic security documents. This report, firstly, describes and explains how the concept of comprehensive defence is represented in each country's defence strategies and the key themes that emerged from that. Secondly, it presents a comparative analysis of the results of the study.

Given that the study used only publicly available sources, it is also important to note that public discussion of national security strategies and the accessibility of strategic documents can both be viewed as elements of national defence strategy. For example, India's national defence documents do not contain a unified statement of its strategies but do emphasise that several states – Pakistan, Russia and others – have made theirs public. In other words, the public disclosure of national defence strategies and strategic documents (often including English translations of framework documents) may form part of a state's deterrence strategy. Both the existence and the absence of public documents can therefore be interpreted indirectly as components of a state's national security strategy.

To meet the aims described above, the study addressed the following research questions:

1. How is the concept of comprehensive defence defined and used in the strategic documents of different countries?

2. What processes do these states follow when developing their comprehensive defence strategies, including those components that pertain to internal security?

3. What lessons or recommendations can Estonia take when developing the internal security component of its own comprehensive defence strategy?

The study involved the following research tasks:

1. Analysing the concepts, development processes and scope of the comprehensive defence strategies of the states included in the study.

2. Comparing those countries' approaches to comprehensive defence from the perspective of internal security and strategy development.

3. Identifying recommendations for Estonia with regard to its strategy development process and the internal security component of its comprehensive defence strategy.

The study examined the following countries:

1. **EU Member States and Nordic countries**: Sweden, Finland, Denmark, Norway, Iceland, Latvia, Lithuania, Poland, Austria, Spain, Germany, Italy, Greece.

2. **Other European** countries: the United Kingdom, Switzerland.

3. **Other** countries: the United States, Canada, Japan, South Korea, Singapore, Indonesia, Taiwan (Republic of China), Australia, New Zealand, India, Pakistan, Saudi Arabia, the United Arab Emirates, Israel, Türkiye, the Republic of South Africa, Brazil, Mexico, Argentina.

All the non-European countries selected for inclusion in the study employ a comprehensive defence strategy that builds on or resembles the original Nordic total defence approach (sometimes described as total or whole-of-society defence) – for example, Indonesia, Singapore and Taiwan. This selection of states was also intended to reflect the defining characteristics of the world regions they are situated in, taking into account, among other factors: strategic and geopolitical position (for example, the presence of a neighbouring state that threatens a state's sovereignty), type of governance, and the role of the military. The aim of using such a broad sample of states was twofold: first, to provide as complete a picture as possible of the practices of states that apply comprehensive defence concepts. Second, to identify factors that a comparison of only small states, similar to Estonia, might miss, yet that would be important to recognise, analyse and consider in specific fields.

For each of the countries included, the study considered the following factors:

1. Does the state have a comprehensive defence strategy, and what are the main documents currently regulating national defence?

2. How is the concept of comprehensive defence interpreted by that state? (This also includes the interpretation of other terms. In some states, the English-language terms comprehensive or total defence are used in their comprehensive defence concepts. In the latter case, the term may refer not only to comprehensiveness in the sense of including more than the military dimension but also to a situation where the military has "total" control or responsibility for national defence.)

3. What are the key areas of internal security in that state? Are they explicitly distinguished in strategic documents, and if so, how?

4. What are the processes through which that state's comprehensive defence strategy is developed, implemented and improved? How are risks and threats translated into priorities? What are the principal areas of focus (pillars) in that strategy? Which authority is responsible for delivering these objectives, and how are they defined? At what intervals is the strategy updated? Does the electoral cycle affect the development and revision of the strategy? (For example, in some states, strategies are developed independently of the electoral cycles, while in others, they have a significant impact on the process and timelines for developing key strategies and priorities.)

5. Does the state employ an evidence-based approach to developing its strategies, and how is this represented in strategy and strategy development processes?

6. Does the state have a system of alternative service? If so, what does this entail, and is that service (particularly in Europe) understood as part of comprehensive defence?

7. What additional findings and possible recommendations can be identified for Estonia?

In addition to the qualitative study described above, a quantitative analysis including Estonia and all 34 countries from the sample was conducted to identify common indicators among states that implement comprehensive defence strategies. The depth of this analysis varied between states, depending on the extent to which their national security strategy documents are publicly accessible.

1. A MAPPING ANALYSIS OF NATIONAL DEFENCE STRATEGIES

NORDIC AND BALTIC STATES

Finland

Finland is often regarded as an exemplar of the modern total defence model. Finland was early to recognise that political independence would be durable only if underpinned by defence self-reliance. During the Cold War, Finland developed its national defence ecosystem in such a way that it became an integral part of societal functioning more broadly. This remained the case after the Cold War. The armed forces retained largely the same structure as before, and the concept of total defence continued to be of central importance to the state. This approach persists today, and Finland's model of total defence based on cooperation across different sectors and engaging society as a whole in national defence is both widely recognised and, in many respects, unique internationally (Wither, 2020, p. 64).

> The main factors identified as affecting Finland's internal security include citizens' societal disengagement, integration, digitalisation, cybersecurity, infrastructure security, energy security, infectious diseases, food security, environmental security and natural disasters.

Today, Finland's defence strategy (*kokonaismaanpuolustus*, "total national defence") includes establishing detailed operational plans and policy measures for maintaining and improving internal security. These were outlined in the 2016 report *Valtioneuvoston selonteko sisäisestä turvallisuudesta*, which identifies citizens' societal disengagement, integration, digitalisation, cybersecurity, infrastructure security, energy security, infectious diseases, food security, environmental security and natural disasters as the principal internal security factors (Sisäministeriö, 2016, p. 53). The need to counter hybrid threats is also acknowledged. In this regard, a key strategic objective is to strengthen the Finnish Border Guard, which is the only institution in Finland with both the capacity and the legal mandate to address both internal and external threats. Recommendations include amending the legal framework to grant the border guard additional capabilities, reinforcing the eastern border, increasing staffing levels (the human factor is considered irreplaceable and there are plans to create a crisis reserve force consisting of retired border guards) and modernising surveillance, including AI-enabled systems (Sisäministeriö, 2016, pp. 40, 51–52). To strengthen the state's disaster-prevention capabilities, meanwhile, the document recommends improving coordination between emergency

medical services and fire and rescue services, which, among other things, would demand investment in upgrading communication systems and organising relevant training exercises (Sisäministeriö, 2016, pp. 42–44).

A second report published by the Finnish Ministry of the Interior in 2016, *Sisäisen ja ulkoisen turvallisuuden keskinäis-riippuvuus*, analysed the relationship between the country's internal and external security needs. The recommendations included increasing the flow of information between the authorities responsible for internal and external security (Tiimonen & Nikander, 2016, pp. 71, 80); identifying shared interests and objectives between these authorities (Tiimonen & Nikander, 2016, pp. 19, 82); developing flexible models for cooperation between internal and external security agencies (Tiimonen & Nikander, 2016, pp. 25, 76, 80); increasing the flexibility of decision-making processes (Tiimonen & Nikander, 2016, pp. 82–83); modernising training by including joint inter-agency exercises; and updating the corresponding legal framework (Tiimonen & Nikander, 2016, pp. 77, 83). In 2017, the Finnish Ministry of the Interior published the security strategy document *Hyvä elämä – turvallinen arki*, which sets making Finland the safest country in the world as the strategic objective and identifies seven trends in Finland's internal security relevant to achieving that goal (Sisäministeriö, 2017, pp. 30–33):

- Social polarisation;
- Fragmentation of "shared values";
- Immigration;
- Extremism;
- Technological development;
- Shrinking public resources;
- Global crises.

The following strategies for responding to these trends are recommended (Sisäministeriö, 2017, pp. 35–49):

- Improve Finland's internal security analysis capabilities, including establishing a new unit that would collect, analyse and report information relevant to internal security as well as monitor internal security threats.

- Enhance the capabilities of agencies engaged in internal security. This would include relevant legislative measures; establishing police and border guard reserves; raising the minimum competency levels among internal security personnel; procuring necessary systems and equipment; increasing border control and surveillance; developing new operational models and scenarios (including with the involvement of private companies); conducting an audit of the Ministry of the Interior's civil defence capacity; developing strategic communications; and opening new communication channels that would engage civilians in internal security.

- Streamline cooperation between the justice system and public services. This would include developing operational models to prevent crime resulting from social exclusion, especially among young people; promoting data sharing between the pri-

vate and public sectors; involving older people in internal security; and maintaining good relations between communities.

- Improve crisis resilience. This would include creating an action plan for improving the crisis resilience of the population through cooperation with NGOs; developing operational models for individuals and institutions; improving the crisis resilience of young people; and developing research capabilities in the field of terrorism. Modernise security systems through establishing an internal security innovation programme in cooperation with the private sector and innovations in the preparation of state-funded projects for the private sector.

- Improve management processes in internal security, including setting inter-agency goals and developing more efficient procedures for recruiting specialists.

- Develop internal security at the local level. This would include drafting recommendations for incorporating internal security into local government strategy documents; identifying appropriate measures of internal security at the local government level; and developing internal security cooperation bodies at the municipal level that would include local governments, private companies, educational institutions and non-governmental organisations.

- Improve monitoring capabilities, including developing an internal security information system led by the Finnish Ministry of the Interior that would function as a cooperation platform for security experts, state authorities, entrepreneurs and NGOs.

In 2019, the Finnish Ministry of the Interior published an implementation report summarising the activities to that date undertaken to achieve the objectives laid out in the 2017 strategy document (Sisäministeriö, 2019).

Based on the information available, it appears that Finland has no specific deadlines in place for updating public strategies related to internal security. Instead, documents are updated on an ad hoc basis, considering evaluations of the results of previous programmes or strategies.

While none of the strategies examined here discussed the Finnish alternative service, the Estonian Academy of Security Science's 2023 report *Application of Substitute Service to the Goals of Estonia's Defense and Crisis Capability* explains that in Finland, alternative service is mandatory for those who do not complete (military) conscription. Those who enter alternative service must undergo basic national defence training so that they become competent to contribute to the state's total defence activities. Alternative service can be carried out at almost all state bodies, including local governments, religious institutions, social services, and most NGOs, including professional associations. The most common service placements are at kindergartens, nurseries, libraries, universities, nursing homes, ministries, churches, cultural institutions, schools and hospitals (Koort *et al.*, 2023, pp. 7–8).

Recommendations for Estonia based on Finland's example:

- Integrate impact assessments and analyses of the results of previous programmes and action plans into the preparation of new strategies to ensure continuity and the use of lessons learned in future policymaking.

- Establish or strengthen a dedicated unit that would collect and analyse internal security data and contribute to evidence-based decision-making and strategy development.

- Improve analysis and monitoring capabilities, establish formats for regular cooperation with universities and research institutions to support evidence-based decision-making and strategy development.

- Enhance the processes for regular information exchange between internal and external security agencies, for example, by establishing joint databases or cooperation platforms to reduce information gaps and improve hybrid threat detection.

- Develop clear but flexible procedures for cooperation between internal and external security agencies that can be dynamically updated in response to the evolving threat landscape.

- Grant Estonia's border guard broader powers to respond to hybrid threats and strengthen surveillance and personnel capacity on the eastern border, including creating opportunities for reserve personnel – for instance, by engaging retired border guards.

- Improve hybrid threat detection and rapid-response capabilities, including by deploying artificial intelligence and developing innovative technological solutions.

- Establish or reinforce cooperation platforms for local authorities, NGOs, educational institutions and the private sector that would focus on risk and crisis prevention at the local level.

- Prioritise the problem of social exclusion among young people and develop operational models to target it – for example, cooperation platforms for social workers, the police, educational institutions and NGOs that enable early identification of risk groups and intervention points.

- Provide regular crisis preparedness training for the general public to build comprehensive readiness to respond to crisis situations. This should involve state authorities, civil society organisations and NGOs.

- Include crisis preparedness subjects in school curricula, require school leaders to have basic security-related knowledge, and teach crisis management and risk awareness skills from an early age.

- Establish an internal security innovation or development programme that pools the resources of public authorities, the private sector and potential funders to develop new solutions for strengthening internal security.

- Incentivise project-based cooperation between the public and private sectors in the field of internal security by allowing the private sector access to funding sources for the development of specific solutions.

- Create a cross-government platform that brings together internal security information, projects, studies and news, thereby enabling rapid information sharing, feedback and faster cooperation processes.

Denmark

Denmark's comprehensive defence approach centres on *Totalforsvaret,* "total defence", which remains an ongoing priority in Danish defence policy. Denmark's total defence has four main pillars: the Danish Armed Forces, the Danish Home Guard, the police and the emergency services (Theussen, 2023).

The origins of Danish total defence can be traced to the Second World War, when it became evident that national defence could not be ensured by the military alone, but had to include other sections of society as well (Theussen, 2023). Danish total defence has evolved from relatively narrow civil–military cooperation in the early 2000s into a genuine comprehensive approach that was formally incorporated into Danish policy planning in 2010 with the establishment of the Peace and Stabilisation Fund, led by the Inter-Ministerial Steering Committee (IGSC). As a result, traditional territorial defence became less central, and attention shifted towards international operations to protect Denmark from unconventional threats. In 2016, the Taksøe Report identified three key objectives for Denmark's comprehensive strategy: the coordination of foreign policy, foreign and security strategy; government decision-making through the creation of a national foreign and security policy forum or council; and the inclusion of parliament in related decision-making processes (Theussen, 2023).

Denmark's defence policy is governed by two principal documents:

- *Danish Defence Agreement 2024–2033* (adopted June 2023)
- *Danish Security and Defence towards 2035* (adopted September 2022)

The Danish Defence Agreement 2024–2033 is a framework agreement that builds on the *National Compromise on Danish Security Policy 2022* to set out political guidelines and the financial framework for the next ten years of defence policy. Under the agreement, the governing parties committed to developing a ten-year framework that enables a dynamic response to evolving demands placed on Danish defence and security. It was also agreed that no single party could veto decisions taken by the defence agreement group. Furthermore, the parties to the agreement committed to guaranteeing that, throughout its duration, the strategic direction of Denmark's defence and security policy will be continuously adapted to changes in the security environment and in accordance with a long-term planning horizon (Danish Ministry of Defence, 2023).

The detailed implementation of the agreement is to be discussed on an ongoing basis throughout the term of the agreement, with specific measures to be adopted in separate partial agreements. These measures should be considered within the framework of the agreement's ten-year horizon and should combine long-term defence planning with the flexibility needed to make political decisions in response to changes in the circumstances and requirements of Danish defence during that period. Such conditions may include shifts in the wider security environment or technological developments that alter the nature of the battlefield and thus the operational needs of the Danish Armed Forces. Implementation of the agreement demands continuous analysis of defence and security policy and rapid decision-making. To this end, each partial agreement will specify where immediate investment decisions are required and which areas call for detailed analysis that would provide a substantive foundation for future investment decisions (Danish Ministry of Defence, 2023).

The defence agreement has been criticised for being limited in various ways compared to the approaches of other Nordic coun-

The origins of Danish total defence can be traced to the Second World War, when it became evident that national defence could not rely solely on the military and that broader societal involvement was needed.

SEVERAL DEFENCE STRATEGIES ALSO INCLUDE ENSURING THE CONTINUITY OF STRATEGIC RESOURCES, INCLUDING CRITICAL INFRASTRUCTURE, FUEL AND COMMUNICATION SYSTEMS. PHOTO: PEXELS.COM

tries. In particular, criticism has focused on the approach's basis in sectoral responsibility, whereby each sector and its respective agencies must guarantee their preparedness to maintain critical infrastructure and societal functions during crises or conflict. As a result, the governing structure depends on ad hoc relationships among ministers rather than a dedicated organisational framework. A further point of criticism is that, while the Danish Security and Intelligence Service (PET) advises individual sectors based on its threat assessments, there is no overarching coordination structure. Only the Prime Minister's Office and its emergency management group can redirect the planning and priority-setting of individual ministries (Theussen, 2023).

> The current approach is based on sectoral responsibility, where each sector and its respective agencies ensure preparedness to maintain critical infrastructure and societal functions during crises or conflict. The prevailing structure relies more on a set of ad hoc relationships among ministers than on a dedicated organisational framework.

The current defence agreement also addresses how to strengthen national emergency management to make full use of available national resources and capabilities. Emergency services previously operated under separate political agreements; their inclusion in the current defence agreement therefore signals the growing importance of a comprehensive, society-wide approach to modern security challenges. The agreement also brings cyber threats in both the public and private sectors within the purview of total defence. Since Danish society is among the most digitalised in the world, it is also a prime target for cyberattacks on both public- and private-sector systems, as well as individuals. Such attacks can serve political and economic purposes and, in general, they represent a serious threat to the foundations of democracy. In this regard, the agreement acknowledges that effective cyber defence requires closer cooperation between the public and private sectors to protect critical national infrastructure, including telecommunications, energy, healthcare, finance and transport (Theussen, 2023).

Since 2015, Denmark has also had a separate national information and cybersecurity strategy. The current aim of that strategy (as revised in December 2021) is to strengthen

Denmark's cyber capability (in line with the defence agreement) through four strategic objectives: protecting essential societal functions, enhancing and prioritising skills and leadership, strengthening public–private cooperation, and participating in international operations to counter cyber threats (Theussen, 2023).

The development of the second document governing Denmark's defence policy, *Danish Security and Defence towards 2035*, included an analysis of Denmark's foreign and security policy across ten different domains (The security policy analysis group, 2022):

1. The international community
2. Global climate change
3. Technological development
4. The nature of conflict today and in the future
5. Societal resilience
6. European and transatlantic security
7. The Baltic Sea
8. The North Atlantic and the Arctic
9. Vulnerable and less developed states
10. Asia and the Pacific

The principal goal of the analysis was to develop a framework for understanding present and future threats and challenges and, on that basis, to set priorities for Danish security and defence policy. To ensure accuracy and depth, the analysis was based on background documents and expert group discussions, with a focus on respected economic, demographic and climate forecasts concerning factors that can be predicted within a certain degree of confidence over the coming decades. The analysis distinguished between military threats, non-military security challenges (such as irregular migration) and risks that may develop into threats over time. To help determine their potential impact, different scenarios were each given a probability grade, from unlikely to very likely. This categorisation scheme could then be used as a comparative measure to help define strategic priorities in defence and security.

Although its principal focus is on the development of military capabilities, Danish Security and Defence towards 2035 is explicit that societal security and effective threat mitigation fundamentally depend on the organisation, responsibility and mutual cooperation of different authorities.

Based on the information available on Denmark's comprehensive defence, it can be concluded that Danish strategic planning is informed by evidence-based research incorporating a range of scientific methods.

No information is available on alternative services in Denmark.

Norway

Norway's defence policy is based on the long-term defence plan outlined in *The Norwegian Defence Pledge: Long-term Defence Plan 2025–2036* (Norwegian Ministry of Defence, 2023b). The document proposes adopting a comprehensive approach to defence built around four major goals: enhancing situational awareness capabilities, creating a new naval fleet, strengthening air defence and increasing the size and capabilities of both land forces and the Norwegian Home Guard (*Heimvernet*). Norway follows the principle that strengthening societal resilience to military and non-military threats requires a whole-of-government framework – a total defence approach that involves international cooperation and coordinated efforts between government authorities, businesses and the population. Civil–military cooperation is therefore an integral part of Norway's defence posture (Norwegian Ministry of Defence, 2023b).

The Norwegian Home Guard is one of the six territorial branches of the Norwegian Armed Forces and has a central role in managing Norway's comprehensive defence. Its principal task is to support operational forces in defending the national territory, and its core responsibilities are:

- Protecting territorial integrity;

- Safeguarding critical infrastructure;

- Supporting institutions responsible for national crisis management;

- Strengthening military presence in Norway's sphere of interest in the Arctic (Marek, 2020).

The Home Guard also serves as a key link between the armed forces and civil society. Civil–military cooperation operates through municipal-level defence advisory committees, which have additional responsibilities related to civil and military planning, preparedness and implementation processes in the regions (Marek, 2020).

Another component of Norway's defence infrastructure is the Norwegian Defence Research Establishment (FFI), which works specifically on total defence. Its purpose is to develop security and preparedness solutions for society and provide research-based support for defence and security measures. Thanks to its research, the FFI plays a crucial role in developing integrated defence and national societal security. It also advises public authorities and stakeholders across the full crisis spectrum, within and beyond the defence sector (Norwegian Defence Research Establishment, [*s.a.*]).

Norway's long-term perspective on comprehensive defence is reflected in the document *Future Acquisitions for the Norwegian Defence Sector 2023–2030* (adopted in May 2023), which outlines the key focus areas for Norway's defence industry over the corresponding time horizon (Norwegian Ministry of Defence, 2023a).

During the Cold War, Norway followed a total defence model designed to mobilise civilian resources for military and civil protection in the event of war with the Soviet Union. To that end, by the 1980s, around one million citizens had been assigned to relevant roles, divided evenly between military and civil functions. Plans also existed for large-scale military requisition of private vehicles, buildings, vessels and aircraft. After the Cold War ended, the military was reduced in size and restructured, and the focus of total defence shifted towards societal vulnerability and peacetime civil protection. Since 2014, the Norwegian total defence concept has once again expanded and now encompasses both territorial defence and civil protection, with an emphasis upon mutual support between the military and society (Wither, 2020, p. 66). Although this model involves fewer people and resources than before, civilian support for the Norwegian Armed Forces in both crises and wartime remains at its core (Wither, 2020, p. 67). The principal goal is to establish the capabilities to address a changing security environment where the boundaries between peace, crisis and war have become blurred. This includes having the capabilities to respond to the diverse range of threats and challenges in the contemporary security environment, including increased migration flows, major terrorist attacks, more frequent extreme weather events and cyberattacks. A key mode of cooperation involves partnerships and contracts with logistics companies, industry and other business sectors, designed to function across a broad range of crisis scenarios, from natural disasters and pandemics to security crises and war.

> The principal goal is to establish the capabilities to address a dynamic security environment where the boundaries between peace, crisis and war have become blurred. This includes having the capabilities to respond to the diverse range of threats and challenges in the contemporary security environment, including increased migration flows, major terrorist attacks, more frequent extreme weather events and cyberattacks.

The updated concept focuses on strengthening crisis preparedness and building greater societal resilience, particularly in critical areas of societal functioning. One example of this is a cybersecurity centre based on cooperation between the public and private sectors, which was established in 2019 under the Norwegian National Security Authority. The centre's task is to increase Norway's digital resilience and respond to serious cyberattacks targeting critical digital infrastructure (Saxi, 2023).

> Norway holds that strengthening societal resilience to military and non-military threats requires a whole-of-government approach – the total defence concept – involving international cooperation and coordinated efforts between government authorities, businesses and the population. Civil–military cooperation is therefore an integral part of Norway's defence posture.

Norway does not have a formal alternative service scheme. However, individuals who cannot complete military service for ideological, ethical or political reasons are assigned to roles in the civil defence sector, where they undergo a three-week training programme. Subsequently, they participate in additional annual exercises that last a few days each (Koort *et al.*, 2023, pp. 9–10).

> **Recommendations for Estonia based on Norway's example:**
>
> - Strengthen integrated defence and national societal security by incorporating evidence-based research. Research organisations should provide expert advice across the full crisis spectrum, both within and beyond the defence sector, to support the development of more effective defence and security measures for the

armed forces and civil society, including measures related to civil–military and cross-sectoral cooperation.

- Establish capabilities suitable for a dynamic security environment in which the boundaries between peacetime, crisis and war have become blurred. This includes addressing a diversifying range of threats and challenges, such as increased migration flows, major terrorist attacks, more frequent extreme weather events and cyberattacks. A key form of cooperation should be partnerships and contracts with logistics companies, industry and other business sectors to ensure the functioning of state systems across crisis situations, from natural disasters and pandemics to security crises and war.

- Modernise crisis preparedness concepts in critical societal functions. For example, in the field of cybersecurity, establish a centre based on public–private cooperation to strengthen digital resilience and address serious cyberattacks targeting critical digital infrastructure.

Sweden

Sweden was one of the earliest adopters of the comprehensive defence concept, alongside Finland and Norway. In Sweden, it is conceptualised as "total defence." Under Swedish law, "total defence" is defined as "all activities that prepare society for a state of war" and encompasses both military and civil defence (Wither, 2020, p. 65). In Sweden, as in Norway, the end of the Cold War led to the restructuring of the armed forces and a significant reduction in resources allocated to national defence. However, in 2015, Sweden's defence policy shifted, as the Ministry of Defence began modernising the nation's total defence concept.

Today, Sweden's total defence continues to comprise two components: military defence and civil defence. Civil defence covers the whole of society and aims to build collective resilience in situations of war or the threat of war. Sweden's resilience is strengthened through preparedness among individuals, government agencies, municipalities, regions, private enterprises and non-profit organisations (Government Offices of Sweden, [*s.a.*]b).

By 2017, several major challenges to modernising Sweden's total defence concept had been identified. Central among those: how to mitigate the impact of the growing dependence on electricity supply, information and communications technology (ICT), communication systems, transport, fuel and financial services to maintain essential societal functions in the event of war – including ensuring the availability of food, drinking water, energy and medicines (Wither, 2020, pp. 65–66).

A 2018 government report confirmed that efforts to restore total defence had been underway since 2015 but stressed that work had to begin "from scratch". Restoring total defence will, therefore, be a long-term project faced with many challenges. Reactive, incident-driven crisis management must be replaced with strategic civil defence planning that covers multiple scenarios and contributes to improving the effectiveness of total defence. Total defence relies on the population's willingness to defend the country, their commitment in peacetime, and their resilience and ability to resist under wartime conditions.

At the end of 2024, the Swedish government presented the updated *Total Defence Bill for the period of 2025–2030* and the *Defence Resolution for 2025–2030*. The latter identifies

significantly strengthening Sweden's comprehensive defence capabilities, which would bolster both Sweden's and NATO's security, as a key objective.

The decision adopting the resolution noted that the Russian Federation's war of aggression against Ukraine, in which deliberate attacks on civilian infrastructure and populations have been a consistent feature, is a clear indicator of the kinds of threats facing Sweden and its allies. As a result, Sweden's current national defence goals include improving its capabilities to address and respond to a wide range of threats, including cyberattacks and hybrid attacks.

The explanatory memorandum to the Defence Resolution for 2025–2030 states that the 2015 and 2020 Defence Resolutions provided an overarching framework. In contrast, the 2024 resolution itself sets out to define concrete capabilities across the entire defence system, with special focus on increases in the defence budget to strengthen deterrence and defence capacity. This includes rapid growth in personnel, higher training volumes, an increased number of conscripts completing service, and the procurement of equipment such as air defence systems and ammunition stocks (Ministry of Defence, 2024).

The resolution for 2025–2030 also calls for reinforcing the operational capacity of the military throughout the implementation period. The strategic objectives include completing and building upon the measures adopted in the previous resolution, while new measures for the forthcoming period include strengthening air and naval forces, and enhancing intelligence and military security service capabilities, as well as a plan to increase digitalisation, innovation and research.

Sweden's national defence plan places strong emphasis on contributing to NATO deterrence and collective defence, which will, in turn, contribute to the development of Sweden's own capabilities. This could include, for example, establishing interoperability with NATO's command structure or enhancing Sweden's capabilities to detect, counteract and actively prevent hostile actions.

The role of Sweden's Home Guard in supporting mobilisation and protecting military sites, base areas and public services makes it an essential part of the country's comprehensive defence strategy. Other vital responsibilities include maintaining local ties and sustaining high levels of public support for national defence. The goal for 2030 is to increase the number of Home Guard members and to diversify and modernise unit equipment (Government Offices of Sweden, [*s.a.*]a; Swedish Ministry of Defence, 2024).

Drawing on lessons from the war in Ukraine, Sweden is also taking steps to reinstate civil conscription. Initially, it will be possible to fulfil alternative service obligations in municipal rescue services, with expansion into additional sectors planned to follow later (Koort *et al.*, 2023, pp. 7, 9).

Alongside national capability development, Sweden has a longstanding tradition of research and development in national security, centred on the Swedish Defence Research Agency (FOI), and its national defence strategy is, in general, developed using evidence-based research and future-oriented forecasts.

The following features of the Swedish model stand out:

1. **Systematic and integrated approach**: The Swedish model relies on a multidisciplinary methodology that combines academic research with analysis by experts in the field.

2. **Society-wide preparedness**: Sweden's comprehensive defence framework gives equal weight to public-sector roles and wider societal preparedness.

3. **Critical progress analysis**: Continuous, systematic monitoring of the state of comprehensive defence and a readiness to present results publicly and explain areas for development are central components of the Swedish model.

Recommendations for Estonia based on Sweden's example:

- Create a long-term strategic planning system. Estonia should institute methods similar to Sweden's to analyse global and regional trends and their impact on Estonia's security.

- Based on Sweden's practice of analysing the progress of developing critical comprehensive national defence capabilities, Estonia should develop a systematic approach to identifying capability gaps and explaining them to the broader public.

- Raise public awareness as a means of increasing transparency.

- Integrate academic and international cooperation into the development of national security decisions and policies.

- Develop cross-sectoral planning processes that provide an integrated approach to addressing human development, resources, the economy, governance and conflicts.

Iceland

Iceland has a distinctive defence strategy, characterised by the absence of a standing army and a strong reliance on international cooperation (NATO Parliamentary Assembly, 2023). National security policy is coordinated by the relevant national bodies, and Iceland's practical defence capabilities are limited to the Icelandic Coast Guard, an armed police unit, and contributions to peacekeeping operations.

The main pillars of Iceland's security and defence are its alliance with NATO and the 1951 bilateral defence agreement between Iceland and the United States (Government of Iceland, [*s.a.*]a). The country places particular emphasis on a comprehensive, multilateral approach to security, premised on the idea that security extends beyond territorial defence. Central to this approach is the view that no state can, acting alone, prevent or manage challenges such as the proliferation of weapons of mass destruction, terrorism, international crime, environmental degradation, threats to financial stability, cyber threats, human trafficking, the negative effects of climate change, or poverty. These transnational risks can only be addressed through active international cooperation (Government of Iceland [*s.a.*]a).

In 2016, the Icelandic parliament, *Althingi*, approved Iceland's national security policy. It spans foreign policy, defence policy and public security policy, and provides for the creation of a National Security Council (Government of Iceland, [*s.a.*]b). The council must regularly assess Iceland's security situation and outlook, monitor implementation – including with regard to the comprehensive approach set out in defence policy – and review the policy at least every five years (Government of Iceland, 2023).

Responsibility for functions related to national security rests with government ministries. Ministries, agencies, and public bodies are required to submit reports or data on security-related matters to the National Security Council, as well as information on new developments or other factors affecting Iceland's national security policy or overall security. Government officials and employees of ministries, public institutions and compa-

nies, as well as individuals and representatives of legal entities, are required to attend meetings of the National Security Council if requested (Government of Iceland, [*s.a.*]b).

The *Parliamentary Resolution on a National Security Policy for Iceland No. 26/145* sets out twelve national security objectives. Most concern the development and maintenance of international cooperation (for example, ensuring that Icelandic authorities participate actively in Nordic, European, and international cooperation activities to deepen and further develop Nordic collaboration in security and defence) (Government of Iceland, 2023). The resolution also emphasises that Iceland should maintain the structures, equipment, capabilities and expertise required to address security and defence issues and to meet its international obligations. It sets aims of promoting the protection and uninterrupted functioning of critical infrastructure and strengthening societal resilience to a wide range of threats. It highlights the need to consider risks associated with climate change, natural disasters, food security, health security and epidemics; to mitigate climate-related disruptions to living conditions and habitats; to participate actively in international cooperation to combat climate change; to promote digital sovereignty; and to enhance cybersecurity and information security across all sectors through coordinated measures and cooperation with other states. In addition, the objectives include ensuring that government policy accounts for threats such as terrorism, organised crime, and threats to the constitution, government administration, and telecommunications – including connections with other states – as well as energy security, financial stability and economic security. The resolution also declares Iceland and its territorial waters a nuclear-weapon-free zone, intended to support disarmament and peace (Government of Iceland, 2023).

> Iceland's national security policy covers foreign policy, defence policy and public security policy, and provides for the creation of a National Security Council. The council must regularly assess Iceland's security situation and outlook, monitor implementation – including with regard to the comprehensive approach set out in defence policy – and review the policy at least every five years.

The National Security Council reports annually to the parliament on the implementation of national security policy. If it finds that amendments are necessary, it submits corresponding proposals to parliament. It also informs the parliamentary Foreign Affairs Committee of matters likely to affect national security policy and its implementation (Government of Iceland, 2016).

Iceland's national security policy covers foreign policy, defence policy and public security policy, and provides for the creation of a National Security Council. The council must regularly assess Iceland's security situation and outlook, monitor implementation – including with regard to the comprehensive approach set out in defence policy – and review the policy at least every five years.

> The *Parliamentary Resolution on a National Security Policy for Iceland No. 26/145* emphasises that Iceland should have the structures, equipment, capabilities and expertise necessary for addressing security and defence issues and for meeting its international obligations. It also sets the aims of promoting the protection and uninterrupted functioning of critical infrastructure and strengthening societal resilience to all types of threats.

The *Parliamentary Resolution on a National Security Policy for Iceland No. 26/145* emphasises that Iceland should have the structures, equipment, capabilities and expertise necessary for addressing security and defence issues and for meeting its international obligations. It also sets the aims of promoting the protection and uninterrupted functioning of critical infrastructure and strengthening societal resilience to all types of threats.

Latvia

Latvia frames its national security approach around comprehensive defence. The key document is the National Defence Concept (NDC). Parliament approved the current NDC in 2020; it outlines the strategic direction for the country's national security institutions. Under the NDC, Latvia's comprehensive defence rests on eight pillars (Latvijas Republikas Aizsardzības ministrija, [*s.a.*]a):

- Maintaining essential state functions;
- Societal resilience;
- Protection of the information space;
- Sustainability of the national economy;
- Engagement of non-governmental organisations and religious institutions;
- Civil resistance;
- Cybersecurity;
- Youth education.

Latvia continues to develop and refine its comprehensive defence approach. Under the *Law on National Security*, the Cabinet of Ministers must submit a proposal for the NDC to parliament no later than 1 October of the second year of each parliamentary term. Article 29 of the same law obliges the Ministry of Defence to draft the new NDC based on the assessment of current military threats. This planning and policy document defines the strategic goals, principles, priorities and measures for three phases: peacetime, escalation and war. It also specifies necessary operational measures and sets resourcing priorities for the development of national armed forces, alongside preparedness measures for other government authorities, agencies and private individuals across these phases. Implementation of the NDC is highly decentralised: the national armed forces implement the plan based on the resources and capabilities available to them as defined by law, while other authorities are responsible for effecting the aspects of the NDC that fall within their respective mandates (Bērziņš, 2023).

The first NDC was approved in 1995, one year after the negotiated withdrawal of Russian armed forces from Latvia. The second version was adopted in 2001 and identified Latvia's principal security challenges as geopolitical factors, economic development, historical foreign relations, education and culture, military and civil defence capabilities, and the environment. The 2020 NDC identified the four core components of Latvia's defence as its national armed forces, the comprehensive defence system, NATO collective defence and international cooperation (Bērziņš, 2023).

Latvia's comprehensive defence strategy has two goals: societal resilience in peacetime and national defence during conflict. It is based on the premise that society, together with national economic structures, must help the armed forces to ensure the continuity of essential state functions, including by providing material support for the armed forces (Latvijas Republikas Aizsardzības ministrija, [*s.a.*]b).

In 2016, Latvia began preparing and implementing the comprehensive defence system strategy set out in the document *About the*

Latvia's comprehensive defence is based on eight pillars:
- Maintaining essential state functions;
- Societal resilience;
- Protection of the information space;
- Sustainability of the national economy;
- Engagement of non-governmental organisations and religious institutions;
- Civil resistance;
- Cybersecurity;
- Youth education.

LOCAL DEFENCE INDUSTRY DEVELOPMENT IS HIGHLIGHTED IN SEVERAL DEFENCE STRATEGIES, BOTH TO ENSURE MILITARY SECURITY AND TO STIMULATE INDUSTRIAL AND ECONOMIC GROWTH. PHOTO: PEXELS.COM

Implementation of the Comprehensive Defense System in Latvia. This document defines seven main strategic objectives and the core responsibilities of the sectors and stakeholders deemed relevant to achieving those objectives (Bērziņš, 2023).

Under the NDC, the Ministry of Defence is responsible for identifying sector-specific threats and for assessing and managing the corresponding processes at the level of sectoral ministries. Sectoral representatives must cooperate with the ministry in developing and approving threat-assessment methodologies and planned policy initiatives. All ministries, the government office and the Cross-Sectoral Coordination Centre must assess and specify the actions and bottlenecks involved in implementing the comprehensive defence model within their respective sectors. Public participation must be as broad as possible when shaping these assessments, including sector-specific public discussions and other forms of consultation, for example, with the Association of Local and Regional Governments, the Employers' Confederation of Latvia and other non-governmental organisations (Latvijas Republikas Aizsardzības ministrija, 2023).

On 19 April 2023, the *State Defence Service Law No. 75* entered into force. The law reinstated compulsory national service, which had been abolished in 2006, and introduced regulations concerning alternative service and voluntary service. The motivation for taking this step was the war in Ukraine and the corresponding need to strengthen national defence capabilities. The law establishes two forms of conscription: military service and alternative

> All ministries, the Government Office and the cross-sectoral Coordination Centre must assess and specify the actions and bottlenecks involved in implementing the comprehensive defence model within their respective sectors. Public participation must be as broad as possible when shaping these assessments, including sector-specific public discussions and other forms of consultation, for example, with the Association of Local and Regional Governments, the Latvian Employers' Confederation and other non-governmental organisations

(state) service. The latter consists of an eleven-month service within certain institutions under the Ministry of Defence for conscripts who, for religious, ideological or other reasons, cannot perform regular military duties (Article 3(2); Article 20) (Fremer, 2023).

TABLE 1. COMPREHENSIVE NATIONAL DEFENSE GOALS IN LATVIA (COMPILED BY THE AUTHORS BASED ON THE LITERATURE)

Strategic objective	Related sectors/ stakeholders	Task
Develop military capabilities and define the defence strategy	Defence sector; National Armed Forces	Develop military capabilities and defence strategies; increase individual preparedness to contribute to national defence and resist occupation
Establish closer co-operation between the public and private sectors	Whole of government	Identify and mitigate threats through whole-of-government measures; cooperate with non-governmental organisations and ensure their participation in national defence; develop national and local volunteer networks; organise annual defence training for professionals and experts across sectors; develop the national defence industry and increase its role in national defence
Defence education in schools and raising public awareness of defence issues	Education and research; defence sector; other government bodies	Implement the national defence curriculum; introduce defence-related subjects in higher education and applied sciences; strengthen the relationship between the state and society
Civil protection and disaster management	Internal security; national and local government bodies; legal persons and private individuals	Implement the seven NATO baseline requirements for civil resilience; strengthen civil–military relations; increase public preparedness to cope with disasters or the initial stages of war
Psychological defence	Government office; defence sector; education and research; culture; other government bodies	Increase societal resilience to influence operations, information operations and psychological operations; strengthen social cohesion; enhance social participation in domestic and social processes; establish direct channels of communication with religious organisations
Strategic communication	Government Office; other government bodies	Encourage the population to act in accordance with the comprehensive defence model; manage government crisis communication; increase resilience to information activities targeting Latvia
Economic sustainability	Finance; economy	Guarantee the provision of essential government services in crises and war; establish national-level stockpiles of essential goods; ensure continuity of operations during crises and war; safeguard economic security

Recommendations for Estonia based on Latvia's example:

- Establish rules to ensure that there is a continuous process of developing and improving Estonia's comprehensive defence.

- Require all ministries, the Government Office and cross-sectoral coordination centres to assess and identify the actions and bottlenecks involved in implementing the comprehensive defence model within their respective sectors.

Lithuania

The core principle of Lithuania's defence policy is total defence. This includes the development of military capabilities and the preparation of state institutions and citizens for potential crises through mobilisation planning, cybersecurity measures, and efforts to strengthen the societal will to defend. Under Lithuania's concept of total defence, all resources and instruments – military and non-military – are mobilised to defend the state (Ministry of National Defence of the Republic of Lithuania, 2023):

- Lithuania is defended by the military and other institutions forming part of the defence system.
- National defence efforts are reinforced by collective defence – the military defends Lithuania alongside NATO allies.
- All civil authorities contribute to defence by supporting the armed forces and ensuring the continuity of essential state functions.
- Citizens defend the country with arms and participate in unarmed civil resistance.

Lithuania's two main current defence documents are the *National Defence Enhancement and Development Programme* (2024) and the *National Defence Plan*, adopted on 6 November 2023. The *National Defence Plan* covers armed defence, mobilisation and civil resistance. In addition to military issues, it also defines the involvement of public servants, non-governmental organisations, businesses and all citizens in Latvia's defence (Morwinsky *et al.*, 2024)

> The current consensus is that total defence encompasses more than preparing for conventional warfare. The best defence is achieved by striking a smart balance between military capability, strong alliances and a society that stands firmly behind its armed forces.

Since 2014, Lithuania's approach to defence readiness has undergone three conceptual phases. From 2014 to the end of 2015, the dominant narrative was that of hybrid warfare. This was followed by debates on the Suwałki Corridor. From 2018 onwards, the concept of total defence has gained momentum and become increasingly central in both debate and policy (Bankauskaitė and Šlekys, 2023). The shifts since 2014 can be broadly grouped into political-legal, political-military, international lobbying (including countering informational threats) and political-administrative areas (including cyber and energy). The current consensus is that total defence encompasses more than preparing for conventional warfare – the best defence is achieved by striking a smart balance between military capability, strong alliances and a society that stands firmly behind its armed forces (Bankauskaitė & Šlekys, 2023).

In Lithuania, those who do not complete compulsory military service must perform alternative service (Koort *et al.*, 2023, p. 7).

- Create a balance between the state's military capabilities, strong alliances, a defence-supportive military and society.
- The current consensus is that total defence encompasses more than preparing for conventional warfare. The best defence is achieved by striking a smart balance between military capability, strong alliances and a society that stands firmly behind its armed forces.

THE REST OF EUROPE

Poland

Poland's most recent comprehensive defence strategy document, the *National Security Strategy of the Republic of Poland 2020* (*Strategia Bezpieczeństwa Narodowego*), was adopted in 2020. Its central aim is to build a comprehensive defence system that links the national government and local authorities with educational institutions, businesses, NGOs and citizens, thereby ensuring Poland's protection against both military and non-military threats. Supply-chain security is identified as a tactical priority. To prepare for future epidemics, developing diagnostic capabilities and cooperating with the private sector to ensure access to medical supplies are key goals. Poland also plans to develop a comprehensive civil protection law. Goals also include increasing resilience in the areas of energy supply, food supply, communication networks, warning systems and transport infrastructure (National Security Bureau, 2020, pp. 15–17).

> Poland's central aim is to build a whole-of-society defence system that links the national government and local authorities with educational institutions, businesses, NGOs and citizens, thereby ensuring Poland's protection against both military and non-military threats.

Recommendations for Estonia based on Poland's example:

- Increase the resilience of supply chains and critical infrastructure, and treat supply-chain security as a strategic priority. Enhance cooperation at both domestic and international levels to secure logistics, food, energy, medical and other essential supply chains. Establish flexible systems for managing emergency reserves, ensure local production capacity (including medical and protective equipment), and introduce digital solutions for supply-chain monitoring and management.

- Engage the private sector and research institutions in improving crisis preparedness by strengthening medical and diagnostic capacity through public–private cooperation. Deepen collaboration with biotechnology, pharmaceutical and medical-sector companies and with research and development institutions to build long-term capabilities for rapid crisis response, domestic production of essential protective equipment and the deployment of innovative solutions such as rapid diagnostic systems.

- Develop a unified approach to total defence law (civil protection and national defence law) and have in place comprehensive civil protection legislation that forms a legal basis for addressing military and non-military threats. Consider updating or expanding the relevant legal framework to ensure clear roles, action plans, and rights and obligations in crisis situations. A coherent normative framework would support more efficient response management in the event of different threat-types

(e.g. military, health-related, cyber, natural disasters) manifesting simultaneously or consecutively.

- Increase resilience in the areas of energy, communications and transport infrastructure by prioritising these sectors and increasing investment in enhancing network systems (e.g. energy, communications and transport) and improving warning systems. Diversify energy sources, put in place backup generators, secure communication channels (including cybersecurity measures), and reliable warning and notification systems, and develop the capacity to transport essential goods and people even in emergencies. As a digital state, Estonia should pay particular attention to cyber resilience and ensure the continuity of business-critical services even during major incidents.

Switzerland

Switzerland's most recent security policy document, *La politica di sicurezza della Svizzera,* was drafted in 2021 (preceded by the 2016 edition) and sets out nine strategic objectives, two of which are unique to Switzerland. The remaining seven are potentially relevant to other states as well (Consiglio federale svizzero, 2021, pp. 29–42):

- Increase measures to ensure quicker threat identification;
- Prioritise hybrid threats;
- Improve the accuracy of public information;
- Strengthen cyber defence systems and processes;
- Secure supply chains;
- Enhance disaster response capabilities;
- Increase cooperation between (local) governments and crisis-management bodies.

On the operational side, Switzerland aims to increase the speed of threat identification by developing satellite capabilities (in cooperation with major powers, especially France), optimising information analysis and assigning specialised personnel from Bern to embassies. To detect hybrid threats, Switzerland is upgrading its airspace surveillance systems; revising the structure of infantry and upgrading equipment to reorient infantry units for urban-conflict readiness, as well as improving cooperation between infantry units and the local authorities that they may need to support in such a situation; increasing military cyber capabilities; and accelerating the procurement pipeline for weaponry, particularly high-technology systems. To ensure the accuracy of public information, the federal government is expanding data collection related to potential influence activities (Consiglio federale svizzero, 2021, pp. 5, 29–33)

To secure supply chains, Switzerland intends to analyse which products imported during the COVID-19 pandemic could be produced domestically.

To improve the effectiveness of its cyber defence, Switzerland requires all service providers to report cyber incidents and is increasing cooperation with operators of strategic infrastructure. To secure supply chains, Switzerland intends to analyse which products imported during the COVID-19 pandemic could be produced domestically, introduce export controls on strategic goods, and establish a legal framework for screening foreign investments. To enhance its disaster-response capabilities, Switzerland intends to map the needs for new civil protection facilities, update civil protection plans (e.g.

for nuclear, chemical and biological incidents), and work with existing climate-change scenarios to identify emerging threats. To enhance cooperation between (local) governments and crisis-management bodies, Switzerland aims – drawing on lessons from the COVID-19 pandemic – to reassess institutional roles and responsibilities; improve the integration of private and academic sectors into national crisis management; and better integrate conscripts into crisis-management structures (Consiglio federale svizzero, 2021, pp. 5, 33–41).

To enhance its disaster-response capabilities, Switzerland plans to map the need for new civil protection facilities, update civil protection plans (e.g. for nuclear, chemical and biological incidents), and work with existing climate-change scenarios to identify emerging threats.

Recommendations for Estonia based on Switzerland's example:

- Consider cooperation with international (e.g. European Space Agency, NATO Allies) or regional partners to gain access to real-time satellite intelligence and improve air surveillance. Additionally, Estonia should increase its rapid-response capabilities in both airspace and maritime intelligence.

- Strengthen data exchange platforms used by national intelligence and analysis agencies and implement artificial intelligence and machine learning tools for rapid detection of threat indicators.

- Consider strategically deploying security, intelligence and analysis specialists to embassies to improve operational information exchange and early detection of threat indicators.

- Develop the capabilities of Defence Forces infantry units to operate in both urban environments and dispersed hybrid operations. Modernise weapons, equipment, training programmes and unit structures to meet contemporary hybrid threats.

- Expand cooperation with local governments to ensure the integration of civil and military forces in crisis situations, which would strengthen the protection of the population and their readiness to respond quickly.

- Increase the capacity of state institutions to monitor disinformation, hostile propaganda and influence activities by cooperating with civil society and the media.

- Develop a clear, unified strategy for rapidly debunking disinformation, strengthening official communication channels, and providing training for media professionals.

- Deepen partnerships with the energy, communications, transport, water and food supply sectors to establish a common cybersecurity standard and regular exercise programmes simulating crises.

- Map strategic goods and materials that are difficult to procure from abroad during pandemics or crises and assess whether they could be produced in Estonia or through intra-EU cooperation.

- Develop mechanisms enabling the state to control exports of strategic goods and to screen foreign investment, to prevent critical infrastructure or technology from falling into hostile hands.

- Update civil protection plans, including in the fields of nuclear, chemical and biological protection, and consider creating new facilities or repurposing existing ones.

- Include climate-related risks (such as flooding) in national security policy and ensure preparedness to manage their impacts.

- Drawing on experience from COVID-19, review institutional roles in crisis management to improve coordination between national, regional and local levels.
- Deepen cooperation with businesses and research institutions to draw on specialist expertise in preventing and managing crises.
- Assess options for engaging conscripts as support personnel in emergencies, for example, in logistics, medical assistance or infrastructure restoration.

Austria

As outlined in the document *Austrian Security Strategy 2024* (*Österreichische Sicherheitsstrategie*), Austrian security policy prioritises "the protection of the Austrian population through a comprehensive approach to security" ("Sicherstellung des Schutzes der österreichischen Bevölkerung im Sinne eines umfassenden Sicherheitsverständnisses") (Bundeskanzleramt, 2024, p. 17). The principal threats identified in the strategy include attempts by authoritarian states or terrorist groups to use migration as a weapon, cybercrime and cyberattacks, disinformation campaigns (including AI-based campaigns), and corruption. To prevent hostile actors from manipulating migration, Austria combines active participation in Frontex and improved domestic strategic communications to counter disinformation and manipulation on migration-related issues. To combat cybercrime, Austria is modernising software and databases across government institutions, recruiting additional IT specialists for the police and making increasing use of AI – all of which will help strengthen cooperation between the private sector, universities and ministries.

The principal threats identified include attempts by authoritarian states or terrorist groups to use migration as a weapon, cybercrime, cyberattacks, disinformation campaigns (including AI-based campaigns) and corruption.

To prevent cyberattacks, Austria is introducing minimum cybersecurity requirements for government bodies. The development of cybersecurity solutions is being expanded through greater involvement of the private sector and universities. To ensure a pool of qualified personnel, Austria supports the training of women in cybersecurity in particular.

Recommendations for Estonia based on Austria's example:

- Increase investment in strategic communication to detect and counter disinformation early in both traditional and social media channels. This is particularly important for preventing disinformation campaigns in sensitive areas such as migration.
- Reduce the impact of hostile influence activities through regular outreach and training programmes to raise public awareness, including media literacy training in schools, universities and public-sector institutions.
- Establish minimum cybersecurity requirements for state and local authorities, covering both technical standards and regular staff training.
- Strengthen cooperation with IT companies, start-ups and research institutions to develop and test innovative cybersecurity solutions. This may include joint projects, research and development programmes, and national support measures for new technologies, including AI-based security solutions.
- Increase the use of AI-based tools to prevent cyberattacks, detect anomalies and track the patterns of cybercriminals.

- Introduce a clear ethical and legal framework for the use of AI, taking into account personal data protection requirements and human rights.

- Support training in cyber defence, strategic communication, AI and international security in universities, and through continuing and retraining programmes.

- Emphasise increasing women's participation in cyber- and IT-security fields by offering targeted scholarships, mentoring schemes and educational initiatives that promote gender balance and expand the pool of qualified specialists.

France

France's *White Paper on Defence and Security* (*Livre Blanc sur la Défense et la Sécurité Nationale*) (2013) sets out the country's defence and security strategy during the period until the publication of the next white paper. It defines five strategic functions for national defence: anticipation, protection, prevention, deterrence and intervention. At the core of France's defence and security strategy are the protection of the population and territory and the maintenance of the state's essential functions.

Accordingly, French ministries are required to carry out tactical cooperation activities with local authorities and with strategic public and private companies to safeguard civilians on French territory. The framework for such cooperation is laid out in an inter-ministerial agreement (between the ministries of the interior, foreign affairs, environment, finance, health and agriculture), which assigns each ministry clearly defined responsibilities for crisis situations. The

French ministries are required to carry out tactical cooperation activities with local authorities and with strategic public and private companies to safeguard civilians on French territory. The framework for such cooperation is laid out in an inter-ministerial agreement between the ministries of the interior, foreign affairs, environment, finance, health and agriculture, which assigns each ministry clearly defined responsibilities for crisis situations.

agreement will be followed by a full audit and, where necessary, procurement processes. In addition, the Ministry of the Interior has made it a priority to strengthen cooperation between local authorities and strategic service providers to develop crisis-response strategies. France has also established an interministerial staff structure with national defence functions (*l'état-major interministériel*), and plans are in place to increase its personnel (Ministère de la Défense, 2013, pp. 111–112, 133–135).

Recommendations for Estonia based on France's example:

- Conclude clear agreements between ministries (for example, the ministries of the interior, foreign affairs, environment, finance, social affairs and rural affairs) that define each ministry's role in emergencies. Such agreements should ideally be legally binding or, at a minimum, formal memoranda that ensure responsibilities, procedures and coordination mechanisms are known in advance, and duplication is avoided. Based on these agreements, carry out regular audits to assess readiness and, where needed, make additional procurements to support crisis preparedness.

- Establish permanent cooperation frameworks to ensure that local authorities have a clear understanding of how to act in crises and how to cooperate with national agencies and strategic service providers (for example, in the energy, telecommunications and transport sectors).

- Develop guidelines, simulations and training exercises for local authorities and strategic service providers to ensure operational readiness.

- Consider creating or strengthening regional crisis management centres to serve as coordination hubs between the central government, local authorities and private-sector partners.

- Establish a permanent, standing interministerial staff with a permanent core team responsible for coordinating defence- and security-related activities both in routine conditions and during crises. The role of this staff would include aggregating information, assessing risks, coordinating the actions of different stakeholders and responding to rapidly evolving security conditions. Additionally, it should be possible to expand it as needed in the event of an emergency.

Spain

Spain's updated national security strategy, *Estrategia de Seguridad Nacional* (2021), sets out three strategic national defence objectives (Ministerio de Defensa de España, 2021, pp. 70–71):

- Improve the crisis-response model, with greater emphasis on developing early-warning systems and strengthening inter-agency coordination.

- Increase the focus on the security dimension of strategic economic sectors, including initiating R&D projects to enhance cyber, health and food security and to advance work on AI.

- Improve hybrid-threat prevention, deterrence, identification and response capabilities.

The strategy's implementation plan is set out in Chapter 5 of the security strategy, which focuses on the national security system. Its cornerstone is the National Security Council, whose decisions are executed by the Situation Committee and supported by specialised subcommittees. Spain's national security system is organised around the concept of resilience, which should be central to crisis management at all levels. Coordination between the central government, regions and local authorities is essential, as is cooperation between ministries, the private sector, universities and civil society. The Situation Committee is responsible for ensuring the capabilities to respond to attacks, particularly hybrid attacks, according to the principles of comprehensive defence.

> Spain's national security system is organised around the concept of resilience, which should be central to crisis management at all levels. Coordination between central government, regions and local authorities is essential, as is cooperation between ministries, the private sector, universities and civil society.

The Department of National Security, which operates under the National Security Council, gathers information on threats from all competent bodies. When a threat is identified, a coordinating unit is formed, consisting of representatives of relevant ministries and security agencies. The security strategy calls for more frequent exercises to test the national security system. It also proposes creating a dynamically updated catalogue of strategic resources, compiled through public–private cooperation, to identify necessary resources that could be made available in crises, as defined by the National Security Council. Spain also aims to develop a multi-indicator early-warning system to accelerate national-level responses to threats, integrate threat assessments with strategic analysis, and ensure that essential information is accessible to all relevant stakeholders. To improve coordination across the system, Spain plans to establish a new body responsible for the secure exchange of classified information among national security actors. Additionally, regions and local authorities are to be more fully integrated into the national security system (Ministerio de Defensa de España 2021, pp. 104–108).

Recommendations for Estonia based on Spain's example:

- Strengthen strategic planning and governance by creating a high-level council body that would coordinate Estonia's security policy, make strategic decisions, and introduce guidelines. The council could include representatives from ministries and local authorities, and its decisions would be implemented by specialised working groups.

- Establish a central coordinating unit (e.g. a situation committee) capable of rapidly implementing the council body decisions and involving multiple sectors and agencies.

- Develop a multi-indicator early-warning platform drawing on both national and international data to enable faster threat detection and response.

- Create a joint system for analysis and information exchange that enables early identification of and coordinated responses to hybrid threats (for example, cyberattacks, disinformation, and threats to critical infrastructure).

- Conduct regular cross-sectoral security exercises to test the reliability of Estonia's national security system and the responsiveness of different stakeholders to identify and address security weaknesses at an early stage.

- Compile and regularly update a catalogue of strategic resources (including critical infrastructure, medical supplies, food, fuel and communications equipment) that would be readily available and thereby reduce response times in crisis situations.

Germany

The primary strategic priority in Germany's most recent national defence strategy, *Weißbuch zur Sicherheitspolitik und zur Zukunft der Bundeswehr* (updated in 2016), is the assurance of comprehensive national security (*Gewährleistung gesamtstaatlicher Sicherheitsvorsorge*). The document states that internal and external security can no longer be clearly distinguished, as crises tend to emerge at their intersection points. Accordingly, Germany's aim is to strengthen cooperation between the state, citizens, private owners of strategic sites, telecommunications operators and the media. Its guiding principle is resilience (*Resilienz*), which is understood as the ability to withstand hazardous situations – natural disasters, system failures or deliberate attacks – without compromising the functioning of the state, economy or society (Bundesministerium der Verteidigung, 2016, pp. 48–49). To achieve these objectives, Germany is building an inter-agency network that improves information flows, increases personnel exchanges between institutions and organises exercises involving both state bodies and the private owners of strategic assets (Bundesministerium der Verteidigung, 2016, pp. 58–59).

> Germany's aim is to strengthen cooperation between the state, citizens, private owners of strategic sites, telecommunications operators and the media.

Recommendations for Estonia based on Germany's example:

- Create or enhance central information and coordination centres that link state agencies, defence institutions and the owners of strategic assets, ensuring that critical information reaches decision-makers and crisis responders without delay.

- Promote staff rotation between ministries, agencies and the defence forces to improve mutual understanding and support more joint-up crisis-management practices.

- Regularly map critical infrastructure (e.g. energy, transport, communications, banking, and the health system) and develop clear cooperation processes between the state and infrastructure owners. Establish additional security measures and contingency plans.

- Encourage citizens to participate in voluntary rescue organisations, crisis exercises and digital-hygiene programmes to build awareness and foster a societal "security network".

- Conduct large-scale simulations involving state authorities, municipalities, communications companies and utility providers to test information-exchange channels, decision-making chains and contingency arrangements.

Italy

Italy's national defence strategy, *Libro bianco per la sicurezza internazionale e la difesa* (2015), focuses on preventing kinetic, hybrid and proxy attacks on Italian territory and against Italian citizens. Italy's primary method for implementing this strategy is international cooperation aimed at ensuring a stable external environment. In civil defence, Italy prioritises cyber defence and the development of robust cybersecurity systems and capabilities (Il Ministro della Difesa, 2015, p. 17). Like France, Italy also prioritises safeguarding the security of its supply chains. This includes identifying which production capabilities are vital for the state and ensuring that they remain under national oversight "independently of ownership structures" ("*independentemente dagli assetti proprietary*") (Il Ministro della Difesa, 2015, p. 60).

> Italy seeks to identify which production capabilities are vital for the state and ensure that they remain under national oversight irrespective of ownership structures.

Recommendations for Estonia based on Italy's example:

- Thoroughly map Estonia's critical industrial, food, energy and digital supply chains.

- Develop mechanisms to ensure that essential production capabilities and the relevant expertise remain under national oversight, even if ownership structures change.

- Promote the competitiveness of domestic companies in strategically important sectors and develop state-supported schemes to reduce excessive dependence on external partners.

The United Kingdom

The United Kingdom's *National Security Strategy and Strategic Defence and Security Review* (2015) sets out the country's strategic goals, which – alongside safeguarding the UK's global influence and economic security – prioritise the protection of the population. The principal components of this strategy include military deterrence (including nuclear deterrence), counterterrorism, counter-radicalisation and counter-extremism measures supported by increased budgets for security services; enhancing cybersecurity capabilities; greater efforts to combat organised crime; increased societal resilience to threats; and improved government crisis-management capacity (HM Government, 2015, p. 11).

In practical terms, the UK aims to increase patrols in its territorial waters; invest £178 billion in new military equipment between 2015 and 2025; improve the interoperability of the armed forces with other security structures (the so-called Strategic Command); expand the operational freedom of the military through legal reform; grow the Army's reserve; recruit around 2,000 new security officers; invest £1.9 billion in strengthening cyber defence; build a new cross-agency platform for managing cybersecurity issues; establish a new intelligence branch specialising in monitoring the dark web; improve the fight against illegal firearms; work with the private sector to curb corruption and sanctions evasion; develop a biosecurity strategy focused on threats from pandemics and biological weapons by 2016; increase resilience

> The principal components of this strategy include military deterrence, including nuclear; counterterrorism, counter-radicalisation and counter-extremism measures supported by increased budgets for security services; enhancing cybersecurity capabilities; greater efforts to combat organised crime; increased societal resilience to threats; and improved government crisis-management capacity.

to energy disruptions in cooperation with the private sector; and reinforce state oversight of critical infrastructure (HM Government, 2015, pp. 23–46).

Recommendations for Estonia based on the UK's example:

- Review and, where necessary, update legislation that supports the operational flexibility and freedom of action of the armed forces and security services.
- Establish a clear legal framework for countering hybrid threats, including disinformation, cyberattacks and economic influence operations.
- Continue supporting community-based initiatives to strengthen social cohesion and reduce social isolation that may contribute to radicalisation.
- Train local governments, NGOs and educational institutions to identify early signs of radicalisation and equip them with tools for prevention.
- Create or reinforce a dedicated unit responsible for monitoring the dark web to detect patterns of organised crime, illegal arms sales, drug trafficking and other threats.
- Increase cooperation with international intelligence and law enforcement partners to exchange information on cyber-criminal networks.
- Strengthen cooperation between financial and tax authorities, anti-money-laundering bodies and the banking sector to detect and stop attempts at sanctions evasion and the movement of corrupt capital.
- Make greater use of data analytics and AI tools to monitor large transaction volumes and identify anomalies more quickly.
- Enhance oversight of critical infrastructure (e.g. energy, telecommunications and transport) and improve cooperation with infrastructure operators.
- Develop plans and invest in modernising infrastructure to increase its resilience to cyberattacks, technical failures and natural disasters.
- Conduct regular exercises to test the state's ability to manage prolonged energy outages. These should involve public-sector actors, private companies and civil society.
- Develop a biosecurity strategy covering early detection, prevention and mitigation of risks posed by pandemics, bioterrorism and biological weapons.
- Invest in increasing the capacity of the healthcare system, maintain reserves of protective equipment, medical devices and pharmaceuticals, and improve information-sharing and laboratory-analysis capabilities.

NORTH AMERICA

The United States

While the concept of comprehensive defence is not as widely cited in the United States as in some other countries, it is, nonetheless, fair to describe its approach to national security and defence as comprehensive, integrated and multi-domain. Two concepts in particular function as close equivalents: the *whole-of-government* approach and the *whole-of-society approach*. These gained prominence after the terrorist attacks of 11 Sep-

tember 2001, which motivated the United States to reassess its security and defence postures, as the evolving threats from terrorism and the effects of globalisation made it clear that traditional military defence alone was insufficient.

The *whole-of-government approach* refers to the integration and coordinated action of government departments and agencies in pursuit of shared objectives, rather than operating in narrow, isolated silos. It is based upon tight intra-governmental cooperation and resource coordination to deliver unified, effective and coherent solutions (Aoki *et al.*, 2023, pp. 733–752).

The *whole-of-society approach* extends this principle beyond the state to involve the private sector, non-profit organisations, international partners, research institutions, communities and individuals. According to this concept, therefore, all segments of society should be engaged in addressing security challenges, strengthening resilience, improving response capabilities and supporting long-term national objectives (United Nations Educational, Scientific and Cultural Organization, 2023, p. 173).

Both approaches are reflected in various key national strategy documents, including the *National Security Strategy* (NSS) (The White House, 2022) and the *National Defense Strategy* (NDS) (U.S. Department of Defense, 2022). These documents both emphasise principles aligned with a comprehensive defence posture. For example, the documents highlight that national defence draws on all instruments of national power – diplomatic, informational, economic, military, financial, legal, intelligence and law enforcement – and, therefore, requires a comprehensive, multi-domain strategy that extends beyond military measures alone (The White House, 2022, pp. 10–13).

The 2022 NDS likewise stresses the need to integrate domains, tools and partners to guarantee national security, as in accordance with the principles of comprehensive defence (U.S. Department of Defense, 2022, p. 2).

National defence draws on all instruments of national power – diplomatic, informational, economic, military, financial, legal, intelligence and law enforcement.

The NSS outlines the United States' goals and strategies for addressing global challenges and maintaining American leadership. At its core is the defence of democracy and the rules-based international order, combined with a commitment to tackling global problems in cooperation with partners and allies. The document highlights the need to adapt to rapidly changing geopolitical conditions and safeguard the United States' position as a leading global power (The White House, 2022, p. 1).

In terms of strategic competition, the NSS identifies China as the most significant long-term challenge. China's economic, diplomatic, military and technological influence requires a multi-layered and coordinated response if the interests of the United States and its allies are to be protected (The White House, 2022, pp. 23–25). At the same time, Russia's aggressive behaviour – in particular its invasion of Ukraine – continues to demand strong deterrence and close international unity (The White House, 2022, pp. 25–26).

The strategy also emphasises the protection of democracy and democratic values, and stresses the need to resist authoritarian influence by promoting human rights and the rule of law, both domestically and internationally (The White House 2022, pp. 10–13). This commitment is linked to the necessity of strengthening democratic institutions to bolster societal resilience against authoritarian pressure.

Global problem-solving forms another central pillar of the United States' national security. Climate change is described as an existential threat that demands international cooperation and rapid action to mitigate its impacts and promote sustainability (The White

House, 2022, p. 6). The NSS also places emphasis upon the need to counter health-related risks, including preventing another pandemic and strengthening global health systems to reduce the likelihood and impact of future crises (The White House, 2022, p. 28). Cyber-security and technological development are also considered priorities, with both being of critical importance to national security and economic well-being (The White House, 2022, p. 34).

The security strategy reaffirms the US's continuing stance as a global leader and the importance of reinforcing alliances and international coalitions. NATO remains central, while partnerships in the Indo-Pacific – including initiatives such as the Quadrilateral Security Dialogue (Quad) and the trilateral security partnership between Australia, the United Kingdom, and the United States (AUKUS) – are also seen as crucial means for ensuring international stability and promoting democratic values (The White House, 2022, pp. 10–13)

In terms of economic security, the NSS focuses on enhancing the resilience of global supply chains, investing in domestic industries and infrastructure, and advancing a fair and rules-based international economic system (The White House, 2022, pp. 27–28). These measures all contribute to securing the United States' competitiveness and economic stability.

Finally, in the area of military action and deterrence, the strategy focuses on the modernisation of military capabilities and the development of new technologies. The prevention of conflicts and diplomacy continue to be central to the United States' strategy in this area; however, strong and credible deterrence is seen as having equal importance (The White House, 2022, p. 31), and, overall, it is only in combining these factors that national security and international stability will be ensured.

The process for compiling the National Security Strategy

Several institutions contribute to the NSS, including the Department of State, the Department of Defense and the Central Intelligence Agency (CIA). Each institution provides expertise from its own field, such as diplomacy, defence or intelligence.

The President of the United States carries final responsibility for approving the NSS and submitting it to Congress. The process is initiated by the President and their office, who draw up initial guidelines that reflect the administration's vision and priorities and form the basis for drafting the strategy. The body responsible for developing the NSS is the National Security Council (NSC). The NSC's principal task is to coordinate inputs to the strategy and review the final document. It comprises several working groups composed of the President's national security advisors and representatives of relevant governmental departments and agencies. These groups are responsible for developing and analysing the strategy in detail. The intelligence community and defence institutions conduct comprehensive threat assessments in which key threats and opportunities are identified. The working groups then discuss potential strategies and policies to address the identified threats. Internal consultations survey the views of members of Congress and government officials. External contributors such as academics, think tanks and allies may also be involved where necessary (Congressional Research Service, 2021).

The overall process can be outlined as follows.

1) **Initiation:** The process begins with the President's office drafting guidelines that reflect the administration's vision and priorities.

2) **Coordination by the NSC:** The National Security Council establishes working groups that include representatives from different agencies and departments.

3) **Analysis and input:**

   a) *Threat assessments*: The intelligence community and defence institutions prepare comprehensive threat assessments.

   b) *Policy development*: Possible strategies and policies are discussed that would address the identified threats and opportunities.

4) **Consultations:**

   a) *Internal contributors*: Consultations are held with members of Congress and government officials.

   b) *External contributors*: Academics, think tanks and allies may be involved where necessary.

5) **Drafting the document:** The working groups prepare a draft strategy, which then goes through several rounds of review and feedback.

6) **Approval and endorsement:**

   a) *NSC review*: NSC members review the final draft.

   b) *Presidential endorsement*: The President formally approves the strategy.

7) **Submission and publication:**

   a) *Submission to Congress*: The NSS is submitted to Congress, as required by law.

   b) *Publication*: The strategy is (typically) made available to the public, except for parts containing sensitive information or details.

The Goldwater–Nichols Department of Defense Reorganization Act of 1986, § 603 requires the NSS to be submitted to Congress every year. In practice, the NSS is published roughly every four years or when there is a change of administration. How often the strategy is updated also depends, however, on international developments and the administration's priorities.

Guidance and principles for preparing the National Security Strategy are collected in the document *A National Security Strategy Primer* (Heffington *et al.*, 2019), which explains how strategic objectives, priorities and action plans necessary for national security should be formulated.

The main processes involved in developing a comprehensive national security strategy can be divided into several key components:

1. **Analysing the strategic situation:** The first step in creating a strategy is to assess the current security environment and how it is expected to develop in the future. This includes understanding both the international and domestic context, analysing threats and opportunities, and evaluating the wider strategic landscape. **A strategist must define the problem, identify assumptions** (for example, estimating an adversary's intentions and capabilities, assessing dynamics in the international environment, and anticipating the potential consequences of action or inaction) **and assess constraints** (such as legal or resource constraints) (Heffington *et al.*, 2019, pp. 7–14).

2. **Defining desired objectives:** After assessing the security environment, the strategist must determine the overall objectives – or *end states* – of the strategy. These objectives should be linked to the protection of national interests (such as security, prosperity and values). The process involves setting specific goals and ensuring that political aims are **clear, focused and achievable** (Heffington *et al.*, 2019, pp. 15–18).

3. **Identifying and developing instruments of power:** These refer to the capabilities and resources at the state's disposal and encompass military, diplomatic, economic and informational power. These forms of power are combined and developed in the following ways to achieve strategic objectives:

   a. *Defining the elements of power:* These include natural resources, geography, human capital, the economy, industry, research and development, technology, infrastructure, governance, culture, national will, and international reputation. They form the basis of the state's capabilities. Although these elements may appear distinct, they are in fact closely interlinked and interdependent.

   b. *Developing the elements of power:* The success of the strategy depends on the state's ability not only to maintain the elements of power but also to develop and translate them into the concrete capabilities needed to achieve political objectives. Examples include an educated workforce, access to critical resources, military capabilities and alliances.

   c. *Integrating institutions and instruments:* Instruments of power – including diplomacy, the military, economic measures and informational influence – operate in close cooperation with institutions and actors such as government agencies, international organisations, NGOs and the private sector. **Strate-**

gists must determine which institutions and instruments are best suited to achieving political objectives and ensure that all elements work in concert rather than undermine one another.

d. *Coordination and sequencing:* Implementing strategy requires prioritising objectives according to their importance and allocating resources optimally. All elements of power must be coordinated so they do not undermine one another. For example, diplomacy, military force and economic measures need to be well integrated if objectives are to be achieved. **Strategists must ensure that any supporting instruments do not hinder the application of the primary instrument**.

e. *Continuous assessment and adaptation:* As strategy is implemented, **strategists must continually assess risks and costs and monitor whether the chosen approach is leading to the desired political outcomes**. Where necessary, the strategy should be adapted to respond to new challenges or changing conditions. Success depends on how well the elements of power can be adapted and redeveloped to meet evolving circumstances (Heffington *et al.*, 2019, pp. 19–36).

4. **Designing courses of action:** At this stage, the strategists determine how the available instruments will be used to achieve the desired objectives. **The strategists must coordinate different elements of power – such as military operations, diplomacy and economic measures – to implement the strategy effectively** (Heffington *et al.*, 2019, pp. 37–42).

5. **Assessing costs, risks and outcomes:** A crucial part of the process is the ongoing assessment of the costs associated with the strategy, including financial and other resource costs. This allows for necessary adjustments during implementation to ensure the strategy's long-term viability (Heffington *et al.*, 2019, pp. 43–48).

Recommendations for Estonia based on the United States' example:

- When formulating a comprehensive strategy, apply a *whole-of-government* approach in which all state institutions coordinate their activities to achieve strategic objectives, avoiding duplication and the waste of resources, and complement this with a *whole-of-society* approach by involving representatives of the private sector, research institutions, civil society organisations and communities in both the design and implementation of the strategy.

- Identify the specific resources and capabilities required to implement the strategy and allocate resources in line with agreed priorities.

- Once the strategy has been compiled, ensure it is continuously under review and adapt it as needed to changing circumstances so that it remains current and effective.

Canada

Canada has a comprehensive national defence strategy. Its defence and security policy has undergone significant changes and is formalised in the document *Our North, Strong and Free: A Renewed Vision for Canada's Defence*, which was published in April 2024. The

strategy sets out defence and security objectives with a focus on national security tasks (Department of National Defence, 2024).

The previous strategy document, *Strong, Secure, Engaged: Canada's Defence Policy,* defined the following areas of priority: well-supported, diverse and resilient people and families; long-term investments in enhancing the capabilities of the Canadian Armed Forces and their ability to support peace and security; increased and better managed defence funding; and the global context (Department of National Defence, 2017).

In response to the current situation, a new defence vision has been formulated – *Strong, Secure, Engaged.* This also informs Canada's new approach to defence: *Anticipate, Adapt, Act.*

National security in the Canadian context encompasses national defence as well as the protection of multiple geopolitical, economic and other interests, and influences not only defence policy but also foreign and other policy areas.

Canada's strategic priority is to protect the safety and security of Canadians at home and abroad. Public Safety Canada is a ministerial committee guided by a programme whose main goals are national security, community safety and emergency management. The committee coordinates the work of federal departments and agencies and is responsible for protecting Canadians, their communities, businesses and interests. Public Safety Canada is also responsible for developing policies and advising the Minister of Public Safety and Emergency Preparedness, and it serves as the central coordination point for counterterrorism, critical infrastructure protection, cybersecurity and transport safety. The committee also works with Canadian citizens to ensure that national security efforts reflect and serve the interests of all communities (Public Safety Canada, 2024).

> Canada has formulated a new defence vision – *Strong, Secure, Engaged* – which also informs its new approach to defence: *Anticipate, Adapt, Act.*

Canada has no continuous process for producing its *National Security Strategy* (NSS), and such a strategy has been produced only once, in 2004. As a result, Canadian ministries and agencies lack a shared understanding of national interests and strategic threats, as well as a common plan for linking these elements.

A 2022 study analysing the United States' and Australia's processes for formulating their respective NSSs, as well as their effectiveness in aligning government institutions across all instruments of national power, concluded that a systematic-delegated process, similar to the one in place in Australia, but with the involvement of the whole government, could be suitable for Canada (Riopelle, 2022).

Canada has prioritised the following issues in its security policy:

- Global power competition;
- Violent extremist groups;
- Technological development;
- The cyber domain;
- Economic security;
- Risks associated with climate change;
- Tackling organised crime and money laundering;

Recommendations and areas of interest for Estonia based on Canada's example:

- Draw on collective defence and regional partnerships.
- Review the defence procurement system.
- Every four years, formulate a comprehensive action plan that is aligned with the national security strategy and publish an annual report.

ASIA

Japan

Japan's first post-Second World War national defence strategy, the *National Security Strategy*, was drawn up in 2013 and is now the country's principal security document. The strategy was drafted by the National Security Council and approved by the national government.

The 2013 strategy was extensively revised by three complementary documents, published in December 2022, that now form Japan's core strategic framework: the *National Security Strategy of Japan* (The Government of Japan, 2022a), the *National Defense Strategy* and the *Defense Buildup Program* (Koshino, 2022). As outlined in these documents, the strategy sets out an implementation plan for the next decade (The Government of Japan, 2022a, p. 35). The National Security Council is responsible for carrying out this plan, as well as continuously assessing the security environment to amend implementation plans where necessary. While Japan does not have in place a separate comprehensive defence strategy, its key strategy documents address aspects of civil–military cooperation and societal resilience.

The 2022 *National Security Strategy of Japan* sets out strategic guidelines for protecting Japan's national security in several key domains: diplomacy, national defence, economic security, technology, cyberspace, maritime and airspace (including space), intelligence, official development assistance, and energy, including the energy industry.

The strategy identifies Japan's national priorities as safeguarding sovereignty and independence, ensuring the welfare of the state and its people through economic growth, and upholding universal values such as freedom and democracy. It is based on Japan's security environment and the principal issues arising from it, and sets out core security principles, including maintaining the alliance with the United States; national defence provided by the Japan Self-Defense Forces rather than military dominance; and cooperation with like-minded countries that share similar values.

> The National Security Council is responsible for implementing the security strategy, as well as continuously assessing the security environment to amend plans where necessary. While Japan does not have in place a separate comprehensive defence strategy, its key strategy documents address aspects of civil–military cooperation and societal resilience.

The strategy establishes national security objectives that include the ability to defend sovereignty and independence, maintaining an international economic environment conducive to growth, shaping a new international order through expanded international engagement (particularly in the Pacific region), and developing rules and regulations in cooperation with the international community, including in the context of climate change and infectious diseases.

The strategy also identifies the capabilities that require strengthening for Japan to safeguard its national security – all of which can be understood as core components of a comprehensive defence approach:

1. **Strengthening the economy and financial sector:** economic growth and national security must be pursued in combination with one another.

2. **Fostering social support for national defence:** the state must make sustained and additional efforts to deepen public and organisational (including private sector) understanding of national security and the need to cooperate in safeguarding it, including awareness of both domestic and international security issues.

3. **Expanding intellectual and technological capabilities:** national security requires evidence-based policy and sufficient technological capabilities. This demands closer cooperation between government, business and research institutions on security-related matters to ensure appropriate measures are in place, including those aimed at countering mis- and disinformation.

Japan's security strategy also emphasises the need to further develop capabilities and preparedness across public and private sectors to deal with future infectious disease-related crises. Civil–military cooperation is also a priority, including the use of commercial airports and ports for exercises and cooperation in the air (including space) and cyber domains to protect critical infrastructure such as satellites and communication systems (Koshino, 2022).

The National Security Strategy of Japan, published in December 2022, sets out strategic guidelines for protecting Japan's national security in key domains: diplomacy, national defence, economic security, technology, cyberspace, maritime and airspace (including space), intelligence, official development assistance and energy, including the energy industry.

The *Defense Buildup Program* (16 December 2022) adds that, in the event of a major disaster such as a nuclear accident or natural catastrophe, the Self-Defense Forces will deploy the necessary measures and equipment to ensure an effective crisis response. The programme specifies that exercises will be held to ensure readiness in the vicinity of nuclear power plants (The Government of Japan, 2022b, p. 32).

Japan's *Police Act* (*Article 71*) empowers the prime minister, on the recommendation of the National Public Safety Commission, to declare a regional or national state of emergency to restore public order, and to deploy police forces accordingly, including reallocating police personnel (DCAF, 2011, p. 48).

Recommendations and areas of interest for Estonia based on Japan's example:

- Continuity planning places strong emphasis on cooperation between the public and private sectors, meaning that the need for collaboration with businesses to strengthen national defence is clearly set out, and companies are expected to contribute actively to national preparedness.

- The role of research and the importance of evidence-based decision-making in national defence should be explicitly recognised. Highlighting the value of scientific activity in the strategy also implies the creation of national resources and a clear rationale for allocating them.

South-Korea

Since 2004, South Korea's[1] *National Security Strategy* has been prepared by the Office of National Security. The 2009 strategy, which focused on the consolidation of South Korea's role in global affairs, is intended to provide the framework for subsequent updates (Lee, 2023).

South Korea also carried out a defence reform in 2006 aimed at modernising national defence in the context of the information age and globalisation. In addition to optimising military units and introducing civilian leadership within the Ministry of National Defense, the reform focused on securing and maintaining a long-term defence budget (Yong-sup, 2006).

The *National Security Strategy* serves as a governmental framework document in which each administration presents its own security strategy. The most recent strategy and strategy in force is the *National Security Strategy: Global Pivotal State for Freedom, Peace and Prosperity*[2], issued on 7 June 2023 by the Yoon Suk Yeol administration. Earlier strategies were presented in 2018 and 2014. The 2023 strategy complements and reflects the spirit of the *National Defense Strategy*, which was published by the Ministry of National

---

[1]   At the time of writing, and under current international arrangements, operational control of the South Korean military in wartime remains with the United States.

[2]   At the time of writing, South Korea is experiencing a political crisis and President Yoon has been removed from office.

Defence in 2022. Every two years, the National Defense Strategy Division also prepares a *Defence White Paper*, most recently released in 2022 (Ministry of National Defence, 2022).

The *National Security Strategy* covers both diplomatic and national security matters, including international relations, reunification with North Korea and national defence (Park, 2023). South Korea has not adopted a separate comprehensive defence strategy. However, various large-scale national exercises have been conducted in order to strengthen societal preparedness – particularly in light of tensions on the Korean Peninsula. For example, a nationwide evacuation drill was held in 2023 to practise sheltering procedures (Lendon, 2023).

> Various large-scale national exercises have been conducted in order to strengthen societal preparedness – particularly in light of tensions on the Korean Peninsula. For example, a nationwide evacuation drill was held in 2023 to practise sheltering procedures.

The current security strategy identifies the principal contemporary security challenges as North Korea's military capabilities, strategic competition between the United States and China, the increasingly significant relationship between the economy and security, and emerging threats such as infectious diseases, climate change and cyberattacks. The strategy notes that these threats disrupt everyday life and the functioning of society. Although these challenges demand global action, states also have an increasingly important role in protecting their populations and ensuring self-defence (Office of National Security, 2023, pp. 11–12).

The strategy defines the key national security objectives as protecting sovereignty and territory, enhancing citizens' safety – including maintaining peace and stability on the Korean Peninsula – and strengthening South Korea's position in East Asia.

In addition to diplomacy, defence capabilities and inter-Korean engagement, key aspects of national security that intersect with the concept of comprehensive defence include economic security and responses to emerging security tasks.

In regard to economic security, the state aims to safeguard its economic interests proactively through multi-dimensional public–private cooperation, by taking the initiative in developing international cooperation norms, and by raising issues and proposing solutions in international fora. National and international economic security are treated as closely interlinked. Ensuring international economic security also contributes to the nation's capacity to maintain the functioning of critical infrastructure during supply chain crises, strengthens cooperation between states on the security of critical infrastructure and new technologies, and accelerates action against climate change and the transition to a lower-carbon economy.

> Proactive responses to new security challenges require a resilient crisis prevention system for non-traditional security tasks, the development of an early-warning system and public–private cooperation mechanisms for crisis response, and enhanced cooperation with the international community on challenges related to cybersecurity, climate change and infectious diseases.

Proactive responses to new security challenges require a resilient crisis prevention system for non-traditional security tasks, the development of an early-warning system and public–private cooperation mechanisms for crisis response, and enhanced cooperation with the international community on challenges related to cybersecurity, climate change and infectious diseases.

In addition to compulsory military service, an alternative civilian service scheme exists in principle, although it is limited to the possibility of working as a prison officer. The overall

system does not encourage alternative service, and those who choose it must serve for a longer period than conscripts in the armed forces (see Koort *et al.*, 2023, pp. 14–15).

> **Recommendations for Estonia based on South Korea's example:**
> - Emphasise the importance of cooperation between the public and private sectors in ensuring national preparedness.
> - Highlight the role of the national economy in supporting national defence, including the need to keep defence capabilities up to date.

Singapore

Singapore describes its comprehensive national defence concept as total defence (Government of Singapore, [*s.a.*]), the central message of which is that "There's a Part For Everyone".

Long-termism, collegiality and a degree of paternalistic state intervention – features often associated with the wider Asian cultural context – are foundational to Singapore's development documents. A key premise is that national strategies shall not focus solely on military defence against external aggressors, but also on non-traditional threats to internal security.

Singapore's total defence approach has its roots in the 19th-century Japanese understanding of comprehensive security, though this concept never fully took hold in Japan itself. For comparison, Malaysia adopted a total defence strategy as early as 1986, while Indonesia's 1945 defence law also took a comprehensive approach to national defence (Matthews & Bintang Timur, 2024).

Before Singapore launched its comprehensive national defence plan, the Advisory Council on Community Relations in Defence (ACCORD) was created in 1984 as a civilian-led body to develop defence-related media strategy and raise public awareness. ACCORD brought together members of parliament, business leaders and trade unions, and its work led to the understanding that defence planning should be developed within the civilian rather than military sphere and communicated more broadly to the public. A council to define this plan was established in January 1984.

Singapore first implemented its total defence concept in 1984, drawing on the national defence models of Sweden and Switzerland. The plan introduced that year is one of the earliest modern defence concepts to approach national security in a comprehensive manner.

> Singapore's total defence encompasses softer measures associated with societal resilience, expressed through collectivism and national identity, alongside more classical defence measures linked to the dynamics of industry and technology, which are necessary to the country's defence capabilities.

A defining feature of Singapore's approach is that state defence and development – including social development – progress hand in hand; what matters is achieving synergy between different actors. Singapore's total defence encompasses softer measures associated with societal resilience, expressed through collectivism and national identity, alongside more classical defence measures linked to the dynamics of industry and technology, which are necessary to the country's defence capabilities. By systematically bringing together different sectors of society, the

comprehensive defence plan has made a significant contribution to Singapore's cultural, economic and military development (Government of Singapore, [*s.a.*]).

Singapore's total defence strategy originally consisted of five pillars and is not routinely revised as a whole. In response to international economic and societal developments, a sixth pillar – digital defence – was introduced in 2019. Alongside this digital pillar, there is ongoing debate on adding a seventh pillar of "climate defence", as experts consider Singapore particularly vulnerable to rising sea levels.

The six pillars of the current plan and their central ideas are as follows (Singapore Civil Defence Force, [*s.a.*]):

- **Military defence** is built on a strong Singapore Armed Forces, which protects the country and resists aggression. A key element is that all citizens also contribute to supporting the military.

- **Civil defence** ensures safety and essential services for the entire community so that daily life can continue as normally as possible even during a crisis. It covers the work of the Singapore Police Force and the Singapore Civil Defence Force in managing national emergencies, particularly by maintaining security and safeguarding essential services that meet basic needs and thereby enable society to return quickly to its normal rhythm. In this context, the state provides training to prepare civilians for rescue work, evacuations, shelter management, first aid, damage control, and the management of blood, water and food supplies. All of this is intended to strengthen societal resilience and reinforce public confidence and readiness in national emergencies. Residents are also encouraged to participate in community-focused activities, including volunteer work such as blood donation or voluntary medical support, to strengthen societal preparedness and understanding of how essential services operate.

- **Economic defence** requires the government, businesses and industry to continually contribute to and support the economy. Individuals also play a part as members of the workforce and help to meet development goals. Companies, including industrial enterprises striving to remain relevant and adapt to change, play a particularly important role. Water security has also become a key component of Singapore's economic defence, as the country has long depended on Malaysia for its water supply. Singapore has made major efforts to diversify supply channels and improve storage, treatment and related capabilities.

- **Social defence** is based on the idea that people should be able to live and work together harmoniously and contribute time to the good of the country and community. Central elements of this are maintaining relations and promoting tolerance between different ethnic groups and combating alienation. Ensuring equality between groups is not only morally right but is also a part of the imperative of political, economic and foreign policy to support national sovereignty and social well-being. Inter-religious organisations and cooperation between faiths are also encouraged to strengthen social cohesion.

- **Psychological defence** means that every resident is committed to the country and confident in its future. It is dependent on people's skills and resilience in unexpected societal situations, including crises. Experts have noted similarities between Singapore's conception of psychological defence and aspects of Finland's total defence concept.

- **Digital defence** is built on the principle that every resident is the first line of defence against digital threats. Digital defence, including cyber defence, focuses on raising public awareness of the various dimensions of a post-truth society, particularly in matters of digital and cybersecurity, such as misinformation, phishing attempts, cyberattacks and related risks.

FIGURE 1. SINGAPORE'S TOTAL DEFENCE PARADIGM (MATTHEWS & BINTANG TIMUR, 2024, P. 642; ADAPTED BY THE AUTHORS)
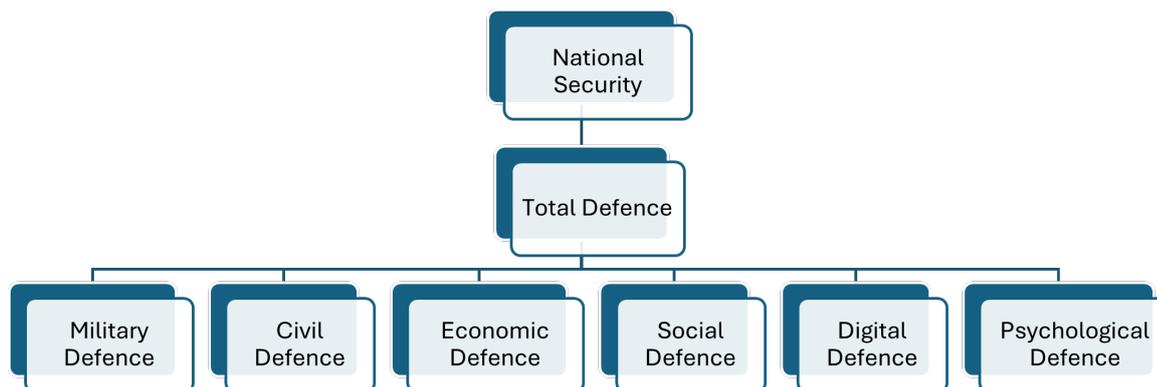
A notable feature of Singapore's total defence concept is its broad scope and the extent to which it involves society as a whole. For example, Total Defence Day is marked on 15 February, the date of Singapore's fall to Japan in 1942, to emphasise the importance of national defence. Educational materials, games and other resources have been developed to introduce the concept to different groups in society, and since 2016, the total defence concept has also had its own theme song.[3]

Recommendations for Estonia based on Singapore's example:

- Involve a wide range of stakeholders in developing a comprehensive national defence concept.

- Develop an overarching concept for comprehensive national defence (similar to the six pillars), designed to be easy to remember and supported by a well-designed visual language.

- Within civil protection, place greater emphasis on training the population to prepare for and cope with crises.

- Strengthen societal attitudes towards national defence through a focus on psychological defence.

- Introduce a range of public initiatives to promote the overarching concept of comprehensive national defence, including learning materials and activities tailored to different population groups.

---

[3]   Theme song video: TotalDefenceSG, 2016.

Indonesia

In Indonesia, the concept of a people-centred defence and security system, known as *Total People's Defence*, has been exploited to serve political power and enforce social control. Crimes against humanity have been committed systematically under its banner, and the same concept has been employed by the Indonesian government and armed forces to justify the creation of paramilitary units made up of civilians for the purpose of maintaining so-called public order.

The Total People's Defense and Security System (*Sistem pertahanan rakyat semesta – sishankamrata*) has been in place since 1945. It was adopted as the official defence doctrine in 1954. The law establishing the doctrine states that national defence is fundamentally the defence of the people. It also sets out obligations for compulsory military service and the reserve duty. The law is implemented by the Indonesian government. At the same time, it has been noted that the country's defence sector, including defence spending, is highly non-transparent (Transparency International Defence and Security, 2020a).

According to the 1973 interpretation of the concept, the responsibility for national security falls to the population – a trained, patriotic and well-organised citizenry (Reza, 2017). The 1982 interpretation emphasises societal resilience and citizens' trust and commitment to the state (Transparency International Defence and Security, 2020a).

Indonesia's defence system, as outlined in the 2015 *Defence White Paper*, is a system of total defence: every citizen has an important role and function in defence. Its foundation is love for the homeland – working together to pursue national interests, including in
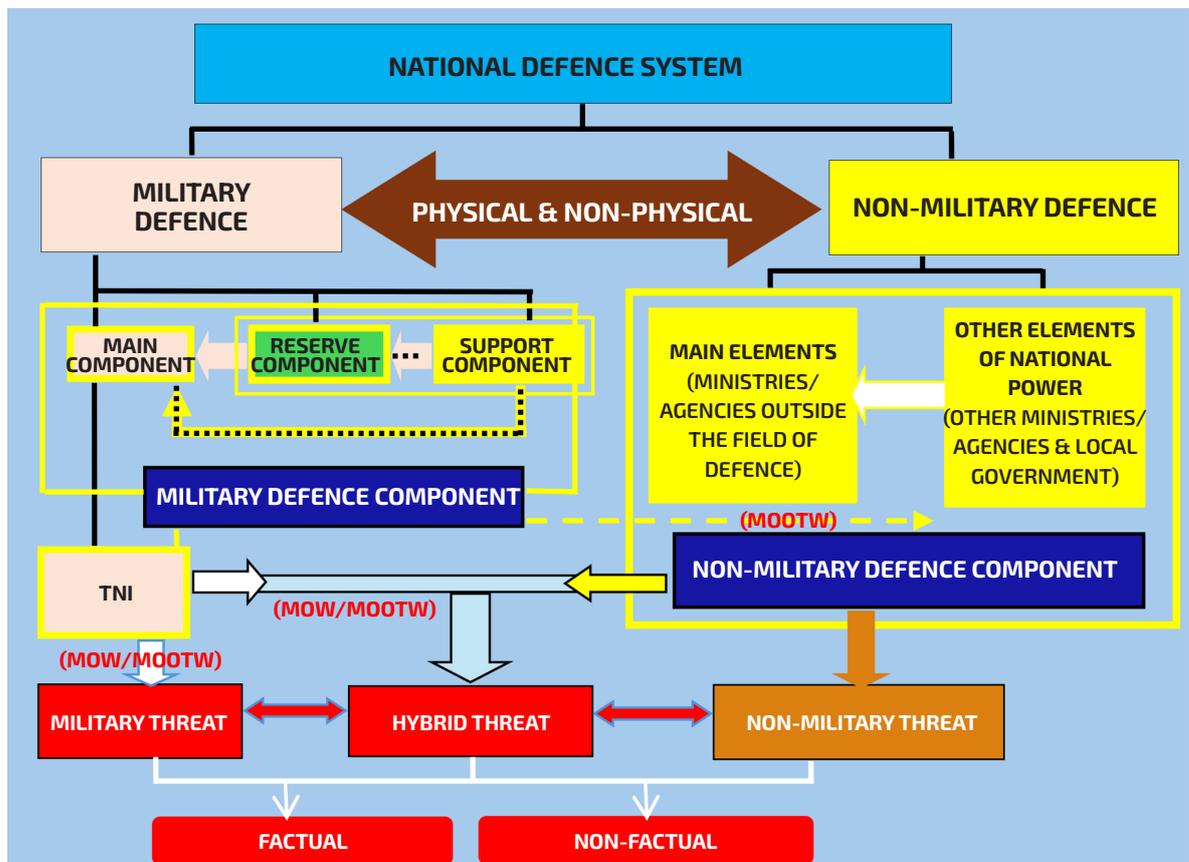

FIGURE 2. INDONESIA'S NATIONAL DEFENCE SYSTEM (MINISTRY OF DEFENSE OF THE REPUBLIC OF INDONESIA, 2016, P. 26; ADAPTED BY THE AUTHORS)

the context of maritime defence. The defence concept serves as guidance for citizens to understand national goals and interests, the nature and structure of defence, its functions and key principles (Defence Ministry of the Republic of Indonesia, 2016, p. 27).

National defence strategy is formally set out in the *General Policy of National Defense*, adopted on 6 January 2021 through *Presidential Regulation No. 8/2021*. It follows an earlier document, *Presidential Regulation No. 97/2015 on the 2015–2019 General Policy of National Defense.*

The *National Long-Term Development Plan (RPJMN) for 2025–2045*, published in 2023, identifies closer cooperation within the security and safety sectors as one of the strategic development priorities in national security (Jiwa Muda Indonesia, 2024), although a detailed description of the cooperation process is not provided.

According to the 2015 white paper, national defence encompasses the state, territory and other resources. Ng and Jasmine (2021) note that in recent years, Indonesia has adopted a new defence concept, *Bela Negara – Defend the Nation*. This term originates from the Total People's Defence concept and is likewise based on the people-centred principle that all Indonesians must contribute to protecting the nation to their own abilities. Given the legacy of military governance under the previous regime, younger Indonesians today remain uncomfortable with militaristic language and tend to prefer a clearer separation between civilian and military spheres (Ng & Jasmine, 2021).

> The foundation of defence is love for the homeland – working together to pursue national interests, including in the context of maritime defence. The defence concept serves as guidance for citizens to understand national goals and interests, the nature and structure of defence, its functions and key principles.

Recommendations for Estonia based on Indonesia's example:

- Value the importance of societal attitudes towards contributing to national defence and make concerted efforts to maintain and strengthen supportive public sentiment.

- Consider and develop a suitable new concept for understanding the historical and semantic nature of national defence.

Taiwan

Taiwan's (Republic of China (ROC)) national defence is regulated by the *National Defence Act*, which was last amended on 6 June 2012.

The Act requires the Ministry of National Defense to publish the *National Defense Report* on a regular basis to explain and clarify national objectives, the international security environment, the state of the armed forces, defence policy, the structure of the defence forces, and provide an overview of military capabilities and resources. The Act also requires the report to reflect the implementation of the concept of *all-out defence* (also referred to as *overall defence*).

Since 2022, compulsory military service for men has been one year (previously, it was four months). Since 2000, it has also been possible to carry out national service in governmental and non-government organisations as well as in social, community or environmental agencies. Alternative service can also be undertaken abroad (for details, see Koort *et al.*, 2023, p. 14).

The most recent report by the Ministry of National Defense is the *ROC National Defense Report 2023*, which was published in 2023.

In addition to conventional military threats (primarily from the People's Republic of China), the report (Lee, 2021) also lists: 1. grey zone harassment, including attempts to normalise incursions into Taiwan's airspace and territory; 2. China's hybrid warfare, such as media infiltration and efforts to foment discord and social tensions through hacking, manipulation of online platforms, the dissemination of contradictory information and propaganda under unity slogans; 3. the "three warfares" – public opinion warfare, psychological warfare and legal warfare – and attempts to manipulate public sentiment and understanding (Ministry of National Defense, 2023, p. 42).

The report also identifies significant non-traditional security threats in the region: emerging infectious diseases, climate change, cybersecurity, energy security (currently, Taiwan imports 98% of its energy) and food security.

Taiwan's strategic objectives are defined as: 1. enhancing national security; 2. strengthening the professionalism of defence personnel; 3. improving self-defence capabilities (including expanding the navy); 4. protecting public welfare through conventional deterrence; 5. deepening strategic cooperation (Ministry of National Defense, 2023, pp. 61–62).

The report also notes that the following methods to strengthen and improve psychological preparedness have been implemented – all of which can be considered aspects of comprehensive defence:

Firstly, a range of media are employed to reinforce patriotism and foster social cohesion, including the *Youth Daily News*, *Endeavor Monthly*, *Sweet Home Journal*, and *Voice of Han* radio programmes and *Jugang Park* TV episodes. The purpose of these programmes is to raise morale and foster psychological readiness among active-duty personnel, reservists and those connected to the defence forces. Military publications, social media posts on platforms such as Facebook and Instagram, and videos are also produced to showcase the results of military training and communicate key messages.

Secondly, the *self-reliant* defence programme includes ministry support for hosting international defence industry events (to strengthen domestic industry, academia and research bodies), multi-year academic and research projects, and the development of dual-use technologies. These activities are partly supported through annual research grants. The Ministry of National Defense has also worked systematically to build public support for defence policy, including by explaining defence industry developments to the public and using a range of different communication channels (e.g. media outreach and personal communications) to raise awareness and strengthen public backing.

The military also plays an important role in civil protection in Taiwan. To this end, it supports *high-availability* rapid response operations, disaster management and epidemic control, protects fishing rights, combats terrorism, and assists in maintaining public order (Ministry of National Defense, 2023, p. 172). During the COVID-19 pandemic, the armed forces supported transport between outlying islands and the main island of Taiwan and helped deliver medical assistance (Ministry of National Defense, 2023, p. 173).

Finally, to build and maintain military–civil unity, Taiwan has introduced the concept of *all-out defence*, which holds that defence concerns everyone and that everyone supports

The Ministry of National Defense has also worked systematically to build public support for defence policy, including by explaining defence industry developments to the public and using a range of different communication channels (e.g. media outreach and personal communications) to raise awareness and strengthen public backing.

and participates in national defence. To reinforce this message, the Ministry of National Defense, with the cooperation of government agencies and local authorities, has hosted numerous activities, including programmes in schools and community education settings (Ministry of National Defense, 2023, pp. 160–161).

Recommendations for Estonia based on Taiwan's example:

- Use media, including new media, to maintain public awareness and readiness to contribute to national defence independently of national reserve training or Estonian Defence League activities.

- Ensure comprehensive defence – or all-out defence – and societal preparedness through cooperation between the state, local authorities and the private sector, for example, by organising training programmes.

AUSTRALIA AND OCEANIA

Australia

The Australian government has published defence white papers that reflect its commitment to national defence and outline its declassified defence strategy for nearly five decades. These white papers have appeared irregularly, though their frequency has increased over the past fifteen years. In 2023, it was recommended that Australia move from periodic white papers to a biennial strategy. The first of these was completed in April 2024 and adopted together with an accompanying investment plan (Dowse, 2024). The latter sets out the specific defence capabilities the government will fund to implement the strategy (Australian Government Department of Defence, 2024a). The aim is to update the strategy every two years.

Australia's national defence strategy sets out the government's approach to addressing the country's key strategic risks within the framework of its defence concept. The 2024 strategy represents a fundamentally new approach to protecting Australia and its interests. Nonetheless, it frames national defence as a task to which the Department of Defence contributes chiefly through the military dimension. Other government departments are expected to continue implementing wider national initiatives, but no government document sets out how these would be coordinated. This has prompted a broader debate in Australia about the absence of a national security strategy, and it has been argued that without a higher-level strategy, Australia may struggle to manage integrated deterrence, devise threat-specific strategies or assess the economic and diplomatic implications of defence policy (Australian Government Department of Defence, 2023).

The coordinated, whole-of-government and whole-of-nation approach outlined in the document is designed to strengthen the following (Australian Government Department of Defence, 2024b):

- Integrated state power.

- National, industrial and supply-chain resilience.

- Innovation, science and technology.

- The workforce and skills base.

- Strong national intelligence capabilities.

Without a higher-level strategy, Australia may struggle to manage integrated deterrence, devise threat-specific strategies or assess the economic and diplomatic implications of defence policy.

The five core objectives of the Australian national defence strategy are (Australian Government Department of Defence, 2024b):

- Protect Australia and its immediate region.
- Deter and prevent attempts by potential northern adversaries to project force against Australia.
- Safeguard Australia's economic links with the world.
- Contribute with partners to collective security in the Indo-Pacific region.
- Cooperation with partners to support the rules-based international order.

Recommendations for Estonia based on Australia's example:

- Defence-related strategies should be assessed and updated at least every two years.
- Invest in innovation, science and technology to help ensure and strengthen national security across different fields.
- Strengthen national intelligence capabilities.

New Zealand

New Zealand's first national security strategy was published in 2023. The strategy sets out a national security vision that promotes a focused, integrated and inclusive approach. The document reflects New Zealand's distinctive geography, history and values, which will form the foundation of the country's future development and position in an increasingly complex world.

The strategy stresses the importance for New Zealand of a peaceful, stable and resilient Pacific region and recognises the value that close international partnerships bring to every security challenge the country faces.

In developing its strategy, New Zealand uses a *Networked Combat Force* approach. This concept links people, sensors, command and control systems (C2), platforms, and capabilities, which are supported by strong organisational structures, business processes, logistics, and infrastructure. The advantage of this approach is its applicability to building operational effectiveness and its suitability to a comprehensive approach to security (New Zealand Defence Force, 2019).

New Zealand's National Security Strategy 2023–2028 is an all-of-government framework that complements various existing strategies and policies, including the *Countering Terrorism and Violent Extremism Strategy*, the *Cyber Security Strategy*, the *Maritime Security Strategy*, the strategy against *Transnational, Serious and Organised Crime*, the *Pacific Regional Plan*, the *Mass Arrivals Prevention Strategy,* the *National Space Policy* and the *Border Sector Strategy* (New Zealand Government, 2023). According to the strategy, the twelve key national security issues most directly affecting New Zealand's national interests are as follows:

- Strategic competition and the rules-based international system;
- Emerging, critical and sensitive technologies;
- Disinformation;

- Foreign interference and espionage;

- Terrorism and violent extremism;

- International organised crime;

- Economic security;

- Pacific resilience and security;

- Maritime security;

- Border security;

- Cybersecurity;

- Space security.

The *Future Force Design Principles 2023* document (New Zealand Ministry of Defence, 2023b) establishes the basis for government decisions on the development of New Zealand's defence forces over the next 15 years. It builds on The *Defence Policy and Strategy Statement 2023* (New Zealand Ministry of Defence, 2023a), which sets out current and future defence policy challenges facing New Zealand.

Although some agencies have national security as their primary mandate, the *National Security Strategy 2023–2028* also highlights that a wide range of agencies work together in their respective areas to ensure a safe and resilient country on a day-to-day basis. Together, these agencies form the national security community, which focuses on protecting the interests of the state and its people.

> Although some agencies have national security as their primary mandate, a wide range of agencies work together in their respective areas to ensure a safe and resilient country on a day-to-day basis. Together, these agencies form the national security community, which focuses on protecting the interests of the state and its people.

New Zealand's defence policy documents are also noteworthy for their clearly structured presentation of objectives, measures and related elements in a variety of thematic areas. One example of this is *The NZDF Strategic Plan 2019–2025* (New Zealand Defence Force, 2019).

Recommendations for Estonia based on New Zealand's example:

- Invest in clearer, better structured and more visually accessible security and defence documents to ensure they reach all groups in society and thereby support a better understanding of the roles and contributions of different actors in safeguarding national security.

THE REST OF THE WORLD

India

India has the world's second-largest military in terms of active personnel and the largest number of volunteer soldiers. The military is governed by the Ministry of Defence of the Government of India. Currently, however, India does not have a public national security strategy or a comprehensive defence concept, and debate over creating such a strategy continues.

The most recent call for a national security strategy was in June 2024, when the Chief of Defence Staff highlighted the need for such a document in the *National Security Doctrine* (Shankar IAS Parliament, 2024).

The doctrine proposes that a future strategy should:

- Set out national defence objectives and outline how those objectives will be implemented and regularly updated.

- Define both traditional and non-traditional threats and opportunities.

- Clarify the responsibilities of different institutions and actors in carrying out these tasks.

Additionally, doctrines and strategies at the national level – including a national defence strategy – must be prepared and approved at the highest levels of government, following the model of the *Nuclear Doctrine*, which was developed by the National Security Advisory Board and adopted in 2023. More narrowly scoped doctrines, programmes and strategies, however, have been drawn up for the military at the strategic, operational and tactical warfare levels, as well as for internal security bodies such as the police.

India has several reasons to develop a national security strategy:

- Defence planning is in poor shape: the system is over-centralised, and strategic guidance is vague.

- Multiple national committees have recommended drawing up a strategy (in 1979, the need for unified deterrence and defence capability; in 2000, the need for major national defence reforms; in 2012, an official national strategy to guide military reforms was established).

- In 2018, a process to draft a national defence strategy was launched, but the results have not been made public. Since then, the United States, the United Kingdom and Russia have all published their national defence strategies, as have India's neighbours China and Pakistan.

The publication of such a strategy is also seen as important since it would:

- Enable the development of a full threat assessment;

- Help align and relate different security and national safety principles, policies and measures;

- Support the allocation and direction of resources;

- Help set clear strategies and priorities;

- Have international significance;

- Help strengthen public and societal awareness and support;

- Help improve cooperation within government on key issues;

- Support national development.

Pakistan

Pakistan is a nuclear-armed state in which, despite its democratic system of government, domestic political instability since 2022 has strengthened the military's role in maintaining political power and societal security (Muneer & Aryal, 2024). While there is no compulsory national service, the country is estimated to have the world's sixth-largest military, and the armed forces continue to expand their presence and cooperation with the civilian sector (Total Military Insight, 2024).

The *National Security Policy of Pakistan 2022–2026* (National Security Division, 2022) was approved by the federal government on 28 December 2021 and is the country's first national security policy document. The drafting process began in 2014 and involved all ministries and agencies, local governments, the governments of Gilgit-Baltistan and Azad Jammu and Kashmir, and military institutions. More than 600 individuals contributed, including members of the National Security Division's advisory council, specialists and civil society representatives. Public hearings on the fundamentals of defence policy were also held in private and public universities.

The security policy introduces a citizen-centred, comprehensive national security framework. Alongside traditional national security sectors, the framework identifies human security, national cohesion and internal security as key pillars.

The policy is based on the concept that national security is shaped by both traditional and non-traditional threats and opportunities. It places economic security at the core of national security and stipulates that: I) economic geography and geopolitics must support national geostrategy; and II) sustained economic growth is necessary to expand national resources. Economic growth is seen as key to guaranteeing the resources needed to safeguard both national and human resources. The principal aim of foreign policy and military capability is to maintain peace and stability in the region and beyond, based on mutual respect and the recognition of an equal right to sovereignty between countries.

> The security policy introduces a citizen-centred, comprehensive national security framework, which identifies human security, national cohesion and internal security as key pillars.

The following activities, measures and aspects identified in the strategy can be considered as components of India's comprehensive national security:

- To ensure national integrity and societal cohesion, it is important to a) promote unity and patriotism while recognising diversity within society and b) promote transparent, efficient and equitable public services, including reinforcing the democratic social contract between citizens and the state.

- To secure the country's economic future, it is important to address three economic challenges relevant to national security: international instability, socio-economic inequality within the country, and geographic inequality between developed and less developed regions. It is also necessary to ensure local energy security and access to international energy supplies through binding agreements. Increasing access to education, including affordability, is also essential.

CLIMATE CHANGE HAS LED STATES TO GIVE GREATER ATTENTION IN THEIR DEFENCE STRATEGIES TO FOOD SECURITY AND ACCESS TO CLEAN WATER, AS WELL AS TO THE CRISES THAT FOOD SHORTAGES MAY TRIGGER, INCLUDING POSSIBLE MIGRATION. PHOTO: PEXELS.COM

The contribution of internal security to comprehensive national security involves:

- All administrative units of the state working toward ensuring the safety of people's lives and property;
- A zero tolerance policy towards terrorism, extremism and violent (minority) nationalist movements;
- Ensuring that the justice system remains effective and people-centred;
- Actively combating organised crime to safeguard the environment necessary for intellectual and economic activity.
- Human security measures that should be taken are:
- Ensure balanced regional development;
- Strengthen food security by expanding farmable land and increasing climate resilience;
- Improve preventive healthcare;
- Adapt to changing climatic conditions and strengthen disaster preparedness;
- Find sustainable solutions to the clean water crisis, including expanding storage capacity.

The strategy further emphasises the importance of countering hybrid threats, including enhancing cybersecurity and information security, and developing space technologies. It also stresses that Pakistan's diaspora should be informed about national issues and actively engaged as part of broader security efforts.

> **Recommendations and points of interest for Estonia based on Pakistan's example:**
>
> - Reduce socio-economic and geographic disparities to support societal cohesion and internal security.
> - Emphasise the contribution of internal security to national defence, including crime prevention, countering extremism and maintaining a transparent justice system.
> - Recognise climate adaptation, including food security, as an essential part of protecting human security and ensuring the continuity of internal security systems.

Saudi Arabia

Saudi Arabia (the Kingdom of Saudi Arabia) – the largest independent state in the Middle East by territory – is an absolute monarchy with no history of elections, no legislature and no parliament. The country also lacks an independent media.

Since the 2010s, Saudi Arabia has expanded its armed forces to address both immediate security threats, including Houthi rebels in Yemen and the influence of IS, and longer-term challenges, such as Iran's growing strength and uncertainty over the extent of US support in the region. Since 2019, women have been able to serve in the military in addition to the police.

From 1932, when the country gained independence, the central aim of Saudi rulers has been to maintain internal order and sovereignty in the face of demographic and economic pressures (including rapid population growth, periods of recession and the decline of purchasing power), rising religious militancy and regional instability. The alliance with the United States has also contributed to domestic tensions. Regime insecurity, including the presence of Al-Qaeda, plays a significant role in shaping Saudi foreign policy (Hoetjes, 2022, p. 5).

There is no publicly available national defence or security strategy. However, some insight into national security governance can be drawn from state documents and international assessments.

Transparency International's *Government Defence Integrity Index. Country Brief: Saudi Arabia* (Transparency International Defence and Security, 2020b) notes that the country's oil reserves and strategic importance have made it a key security partner for both the United States and the United Kingdom. Moreover, Saudi Arabia was the world's largest importer of US and UK arms from 2016 to 2020.

The Crown Prince of Saudi Arabia, who also serves as defence minister, has strengthened his control over the armed forces. Effective authority over defence, therefore, rests with the crown prince, who sets policy and makes budgetary and procurement decisions. At the same time, there is no transparency regarding the processes involved in national security and the use of funds directed to those processes. The military is highly vulnerable to corruption, including in personnel management. The crown prince also relies on

The plan set for 2030 aims to develop the local defence industry not only to reduce defence expenditures, but also to generally boost and advance the local industry, including the production of ICT and industrial technology.

private military companies for security in Saudi Arabia and the wider region, and these entities are not bound by Saudi law.

The Council of Political and Security Affairs of Saudi Arabia, one of two subcabinets of the Kingdom of Saudi Arabia, is nominally responsible for defence matters, but it has no formal oversight powers and limits itself to making recommendations on government decisions, which are rarely contested.

In 2016, Saudi Arabia launched the national programme *Kingdom of Saudi Arabia Vision 2030*, which is built around three pillars: a vibrant society, a thriving economy and an ambitious nation (Kingdom of Saudi Arabia, 2016, p. 13)

The aim of the programme is to develop a domestic defence industry not only to reduce defence spending but also to boost industrial growth more generally, including ICT and advanced manufacturing. Although defence spending is high, currently, only 2% of it is domestic. The country has set the goal of retaining 50% of designated defence expenditure within the country by 2030. To accelerate industrial development, the government is directing state investment to the sector and seeking strategic partnerships with leading global firms. Domestic production is expected to strengthen defence capabilities and advance research and development more broadly (Kingdom of Saudi Arabia, 2016, p. 47).

In December 2020, Saudi Arabia also presented its *National Cybersecurity Strategy* (National Cybersecurity Authority, 2020), which is built around six pillars: coordination – national-level cybersecurity governance; management – flexible national cyber risk management; resilience – ensuring the functioning of the cyber ecosystem; protection –

Domestic production is expected to strengthen defence capabilities and advance research and development more broadly.

strengthening national cybersecurity and technical capacity to respond to cyberattacks; partnership – enhancing cooperation and collaboration in cybersecurity; and development – expanding national capabilities and advancing the cybersecurity sector.

> **Recommendations for Estonia based on Saudi Arabia's example:**
>
> - Develop the domestic defence industry, recognising it as an important component of the national economy. Strengthening local production can support the labour market and improve the wider social situation.
>
> - Build connections between national research activity and the defence industry. A domestic defence sector supports research and development both directly, through innovative solutions, and indirectly by raising the overall level of national research and development.

The United Arab Emirates

Though situated in a politically complex region, the United Arab Emirates (UAE) has secured a firm position on the global political landscape thanks to its resources and strategic location. It is also one of the wealthiest countries in the world in per capita terms, and 8% of global oil reserves lie within its territory. The UAE's most significant standing threats stem from its largest neighbours, Iran and Saudi Arabia. At present, its main security concerns are the Muslim Brotherhood and Iran (Hoetjes, 2022, p. 5).

In addition to the United States, the UAE has important defence partnerships with the five member states of the Gulf Cooperation Council – Bahrain, Kuwait, Oman, Qatar and, in particular, Saudi Arabia. In 2014, an agreement was reached to build a joint military base in Bahrain and a strategic base in Abu Dhabi. The UAE and Saudi Arabia make up the region's leading states, especially following the resolution of conflicts between Ethiopia and Eritrea (MCC, 2024).

The UAE's security is principally based on its political and economic ties with the United States. It is also the only Arab state that has served alongside the US in allied operations over the past 30 years, including in Afghanistan and Libya.

In 2014, a 16-month compulsory military service requirement was introduced to increase the number of reserve soldiers. A number of former US military personnel also serve in the UAE military and as military advisers.

The UAE also draws on its financial capacity – particularly through development and humanitarian aid programmes – to advance its interests and expand its sphere of influence. It employs soft power, including through economic, medical and media resources, both to protect itself from Islamist groups and to present alternatives within the Arab world.

As noted in Transparency International's *2020 Government Defence Integrity Index. Country Brief: United Arab Emirates*, the UAE has no publicly available national defence or security plan. Therefore, defence expenditure is difficult to trace or analyse. At the same time, defence spending is also linked to foreign policy objectives, such as strengthening or maintaining relationships. While arms imports from the United States have declined and imports from China and Russia have increased, the UAE has also developed its own defence industry (Transparency International Defence and Security, 2020c).

In November 2020, the Cybersecurity Council UAE was established with the aim of developing a cybersecurity strategy and a secure and robust national cyber infrastructure. This evolving defence approach reflects the unprecedented security challenges facing many Gulf states, particularly the UAE. These challenges extend beyond military, security and economic issues to social, environmental and technological concerns.

The UAE also draws on its financial capacity – particularly through development and humanitarian aid programmes – to advance its interests and expand its sphere of influence. It employs soft power, including through economic, medical and media resources, both to protect itself from Islamist groups and to present alternatives within the Arab world. Soft power, particularly assistance to neighbouring countries, has been one of the UAE's primary foreign policy tools since the 1980s.

Recommendations for Estonia based on the UAE's example:

- Broaden the list of recognised threats to national security to include environmental risks, which can affect not only migration flows and regional competition over resources but also the functioning of internal security.

- Recognise the novel challenges posed by technological change in its broadest sense, as rapid technological advances have a direct impact on national security and on maintaining societal safety.

Israel

Israel does not have a formal, government-approved national security strategy or doctrine. The need for such a strategy remains a topic of debate, and many argue that Israel

should set out the central pillars of its defence policy in writing. The closest equivalent to a national security strategy is considered to be the extensive 1953 briefing on national security problems presented to the government by Prime Minister David Ben-Gurion, though this was in fact a multi-year situational report. Several attempts have been made to draft a strategy: a committee established to produce an integrated national security concept prepared draft texts, but these were not approved by the government and did not gain political support. Prime Minister Benjamin Netanyahu is reported to have drafted a comprehensive national security concept in 2018. However, while the concept's key ideas have been discussed in publicly available sources, no direct quotations or formal references have been published.

Israel must adapt to a diverse and rapidly changing security environment. Foreign and domestic policy must evolve accordingly and be handled with care and strategic foresight.

In 2019, the former head of the Committee to Formulate Israel's National Security Doctrine (the committee tasked with preparing Israel's security doctrine in 2006) Ron Eldadi and the committee's secretary Dan Meridor published an extensive review of Israel's challenges and possible solutions, but even this cannot be regarded as an official security document (Meridor & Eldadi, 2019).

Although no unified, approved doctrine exists, defence has always been decisive in governing the state and each administration has had its own emphasis.

The Israel Defense Forces (IDF) are the primary body responsible for implementing national security policy. Mossad (the Institute for Intelligence and Special Operations) and the Israeli Security Agency (Shabak) play vital roles, as, in certain areas, do the Israel Atomic Energy Commission, the National Cyber Directorate, the police and the emergency services. More broadly, the Ministry of Foreign Affairs and other government bodies also share responsibility for Israel's international position.

The Jerusalem Institute for Strategy and Security identifies a set of principles that constitute Israel's unwritten but broadly accepted security doctrine (Amidror, 2021). These explain the state's military defence posture but do not address the aspects of comprehensive defence. The principles are:

- Israel makes every effort to maintain its ability to defend itself independently, without depending on allies or partners. The focus is on ensuring that its defensive and offensive capabilities exceed those of potential adversaries. Large portions of the national budget are directed to defence, and public support is vital.

- Israel maximises its military capabilities through conscription and a large standing and reserve force. The length of service is deliberately long to allow for extensive training, and reservists undergo continuous refresher training.

- Israel must maintain deterrence at several levels and be prepared for direct military attack and a range of other existential threats. This includes developing cyber defence and multi-level intelligence capabilities, as well as other deterrence tools.

- Israel must adapt to a diverse and rapidly changing security environment. Foreign and domestic policy must evolve accordingly and be handled with care and strategic foresight.

- Finally, Israel recognises that adversaries will not disappear and, therefore, continuous preparedness is essential.

Military service of at least two years and eight months is compulsory for Jewish men and women, and for Druze and Circassian men. Jewish women must serve at least two years.

Service may also be completed in internal security institutions, through volunteer work or in similar roles (for details, see Koort *et al.*, 2023, pp. 13–14).

> **Recommendations for Estonia based on Israel's example:**
> - Emphasise the constant evolution of the security environment and the need for flexibility in foreign policy, which indirectly points to the importance of having the confidence to adjust direction in response to changes in the wider security environment.
> - Stress the importance of continuity and vigilance in national defence: actors that threaten the state remain present even when their activity is neither active nor visible.

Türkiye

Türkiye (Republic of Türkiye)– which has the second-largest army in NATO – occupies a strategically important position, and its long-standing relations with its neighbours make it a key security actor in Europe, the Balkans, the Caucasus, the Middle East, the Mediterranean and the Black Sea.

In Türkiye, all male citizens aged 21–41 must complete at least six months of military service, and women may also serve, although there is no legal alternative service framework.

In 1990, the military dominated national defence planning, and the civilian government had a say only in the final approval of the strategy. Since 2002, however, civil–military relations have changed significantly: the government became the authority responsible for setting the military and defence agenda, foreign policy moved the defence industry into focus, and the military was forced to adapt to its new situation. Following the failed military coup of 2016, the defence minister became the highest authority in military decision-making. Since 2018, the President has held substantial power over civil–military relations and the shape of Türkiye's defence architecture (Yanan, 2024).

Türkiye's defence and security policy has been transformed over the past decade. The aftermath of the Arab Spring reshaped the security environment at home and in the region, while Türkiye has also sought to shift its global position and prove its military capabilities. National security, including the preservation of the political system, is clearly prioritised over individual security (Tank, 2021).

Although Türkiye's main defence policy document, the *National Security Policy Document* (*Milli Güvenlik Siyaset Belgesi*), is not publicly accessible, there is evidence that the document underwent significant revision in 2022 based on Türkiye's core national values and with little regard for its long-standing allies, the United States and Europe (Yanan, 2024; Bozkurt, 2022).

Türkiye's new military and defence strategy is shaped by domestic, regional and international developments (Yeşiltaş, 2020), and both the decision makers and Türkiye's geopolitical vision have changed. Within Türkiye's civil–military framework, the Turkish Armed Forces hold a special position above politics, and the Turkish military industry enjoys a similar privileged status. The core goal of Türkiye's military and defence planning is strategic autonomy, based on an independent and sustainable defence posture and

defence industry, and the ability to formulate and pursue its foreign, military and defence strategy without relying on allies. Türkiye also seeks a dominant role in its region.

As the Turkish Ministry of Foreign Affairs describes Türkiye's national security approach, the country's security and self-defence are closely linked and have three dimensions: the survival of the population, the preservation of territorial sovereignty, and the protection of national identity as it has developed politically, economically and culturally. Ensuring security, both national and international, goes beyond military capability and policy. Modern security challenges require military, economic, social, political and legislative measures. In short, a comprehensive approach is needed to address contemporary security tasks (Republic of Türkiye Ministry of Foreign Affairs, 2022a; Republic of Türkiye Ministry of Foreign Affairs, 2022b).

Achieving strategic autonomy requires strengthening the military, including its readiness; taking preventive action supported by an already established posture of strength; implementing strategy (for example, in counterterrorism) and maintaining military deterrence, including the presence of troops abroad.

Türkiye also exercises various forms of soft power. Its involvement in Syria since 2011, under the Justice and Development Party (AKP), which rose to power in 2002, forms part of a Turkish approach to humanitarian aid and peace promotion that contrasts with Western policy (Tank, 2021). For neighbouring states, humanitarian assistance has strategic and security objectives; for more distant states, it also contributes to trade and business interests. Providing aid strengthens ties between the countries involved while the donor state is able to acquire significant influence, including in shaping projects in the countries it assists, to further its own foreign policy interests. For Türkiye, humanitarian assistance and peace negotiations are a key part of the AKP's broader exercise of power.

Turkish foreign policy, which is seen as a guarantor of national security, is interwoven with domestic politics and, whether it reflects the agenda of the governing party or the President, is used to bolster domestic standing. Foreign policy failures tend to be seen as failures of leadership.

Recommendations for Estonia based on Türkiye's example:

- Strengthen and emphasise the role of economic, social and political decisions in national defence. In other words, national defence should be directly shaped by the state's overall policies and decisions, not solely by the activities and policies of the Ministry of Defence.

The Republic of South Africa

The defence policy of the Republic of South Africa (hereinafter, referred to as the RSA) is formally defined by the Constitution and supported by strategies issued by the Department of Defence, the national defence white paper *The Defence White Paper* (Government of South Africa, 1996) and the South African Defence Reviews, which are periodic, systematic reviews of the country's defence sector. The RSA has not adopted a separate comprehensive defence strategy or concept.

The South African Constitution (*Schedule 6, section 24 of the 1996 Act*) sets out the tasks of the South African National Defence Force (SANDF), including those pertaining to internal security, as follows:

- Protecting sovereignty and territorial integrity;

- Fulfilling international obligations;

- Preserving and protecting life, health and property;

- Ensuring and supporting essential services;

- Enforcing the law;

- Supporting all state institutions, including ministries and other institutions in their respective areas of administration.

The Constitution of South Africa *(1996, Article 201(2))* also stipulates that the President, and only the President, as head of the executive, may authorise the use of the defence forces in support of the police, for national defence, or to meet international commitments.

In addition, the *Defence Act (2002 [Sec 18(1)])* provides the President or ministers the power to authorise the use of the defence forces domestically or in international waters if doing so is necessary to:

- Protect life, health or property;

- Ensure essential services;

- Support a state institution or area of administration;

- Carry out border control.

The South African Defence Force is a professional military body, and compulsory military service was abolished in 1994.

Parliament has the mandate to approve and revoke defence policy, although this power has never been used. Three parliamentary committees address defence matters: the Select Committee on Security and Justice and the Joint Standing Committee on Defence. In practice, many of Parliament's recommendations to the Department of Defence remain unimplemented, and compliance with audits is uneven. The ministry submits an annual expense budget, but the nature of the expenditures is not always transparent.

According to Transparency International's *Government Defence Integrity Index. Country Brief: South* Africa, published in 2020, the most recent defence review for the RSA was submitted in 2014 (Transparency International Defence and Security, 2020d).

The RSA holds a unique position in international affairs through investment, trade agreements and an active role in the African Union. Despite having one of the continent's most diverse and developed economies, poor governance and declining democratic standards have contributed to economic stagnation, high unemployment and slow socio-economic development. Consequently, the weakened economy has strained the defence sector, which is now underfunded and poorly equipped.

According to the strategic plan presented by the Ministry of Defence in 2020, *Department of Defence Strategic Plan for 2020–2025*, the Department of Defence's vision is: "Effective defence for a democratic South Africa" and its mission is: "To enable, utilise, maintain and renew defence capabilities in accordance with the needs of the Republic of South Africa as stipulated by law" (Republic of South Africa Defence Department, 2020).

The strategy emphasises that national defence architecture must have local, regional and continental dimensions. From a comprehensive defence perspective, the local dimension is central, and human security, sovereignty and priorities related to territorial integrity, constitutional order and well-being, including economic growth and good governance, should all be areas of focus. National security depends on regional and continental security, and economic success depends on peace, stability, growth and the strengthening of democratic values. The defence strategy is intended to support the government's plans in all three dimensions. The Department of Defence is currently assists, and will continue to assist, municipalities and state institutions in both providing humanitarian relief and crisis response, and it also provides support regionally.

Economic success depends on peace, stability, growth and the strengthening of democratic values.

The principal role of the military is to defend the RSA's borders on land, at sea and in cyberspace. Border protection is a matter of national safety and security that requires sufficient resources, in addition to technical and infrastructural support. With a coastline of roughly 3,900 kilometres, maritime security and lawful activity at sea are of critical importance.

The Department of Defence plans the following steps to strengthen defence capability: invest in human resources, including skills development and management training, continue to operate effectively within tight financial conditions, and develop ICT.

Recommendations for Estonia based on South Africa's example:

- Emphasise the role of economic stability and economic growth as a security issue, specifically as a foundation for societal well-being and stability.
- Define the Ministry of Defence's role in supporting other state institutions and local authorities during crises, and ensure that the ministry plans the resources and supplies needed to provide broad assistance when required.

Brazil

Brazil is the world's fifth-largest country by area and seventh by population, with a developing economy. Transparency International's *Government Defence Integrity Index. Country Brief: Brazil* (Transparency International Defence and Security, 2020e) notes that the past decade has seen economic decline, rising homicide rates and major corruption scandals. The election of President Jair Bolsonaro in 2018 was followed by a hard-line security policy, deep political polarisation and attacks on democratic institutions.

Since 2018, the armed forces have been extensively involved in internal security: they have taken over several policing functions, led raids against gangs, committed widespread human rights violations and operated outside legal frameworks. Corruption within the armed forces affects both procurement and management of human resources.

The Brazilian Armed Forces (*Forças Armadas Brasileiras*) are a professional military, but the country also has compulsory service for all men aged 18–45 except clergy (service lasts 10–12 months), and women have been able to serve since 1980 (the first such policy in South America).

The *National Strategy of Defense* was adopted in 2008, and the *National Defense Policy* (*Politica Nacional de Defesa*) dates from the same year. In 2012, the documents were harmonised, and they continue to function in parallel today. The *Defense Policy* focuses on external threats, and while it does not explicitly refer to the concept of comprehensive national defence, it acknowledges that social, political and economic factors contribute to the secure functioning of both the state and society (Política Nacional de Defesa, 2013).

The *National Strategy of Defense* is narrower in scope and primarily defines the military capabilities that are of the most strategic importance to national defence: cyberspace and cybernetics (including production, education and military use), airspace (including satellite development and production) and nuclear capability (while rejecting nuclear weapons, Brazil maintains its broader nuclear competence). A key goal is reorganising the national defence industry to support independent technological development.

Strategic activities that can also be understood as aspects of a comprehensive national defence include:

- Research, development and innovation in support of national security, with close cooperation between the Ministry of Defence and the Ministry of Science, Technology and Innovation, in particular, being an important strategic objective.

- Investing in human resources and promoting the value of military careers in society.

- Educational programmes that involve a range of civilian sectors in defence issues (including more public communication, disclosure, and explanations of defence activities, and teaching defence topics in secondary schools).

- Developing, legislating and implementing basic principles governing mobilisation and demobilisation.

- Improving logistics between actors such as the defence industry and the armed forces.

- Working to align national industrial and infrastructure with the country's national defence needs.

- Revise legislation concerning internal security and law enforcement so that the armed forces can support internal security when required.

- Ensure that all state institutions contribute to national security, for example, by developing a national crisis-preparedness model, improving crisis-response capabilities, strengthening critical infrastructure resilience, supporting public-space security and protecting paramedics.

> The National Strategy of Defense is narrower in scope and primarily defines the military capabilities that are of the most strategic importance to national defence: cyberspace and cybernetics (including production, education and military use), airspace (including satellite development and production) and nuclear capability (while rejecting nuclear weapons, Brazil maintains its broader nuclear competence).

In 2020, an analysis by Siqueira Bricki identified a number of shortcomings in the *National Defense Policy*, *National Defense Strategy*, and the *National Defense White Paper*.

- The documents stress the importance of defence but do not define priority areas, and neither reforms nor capability improvements are analysed without a corresponding increase in defence expenditure.

- They form a plan drafted by the Ministry of Defence without political backing, which is insufficient grounds for implementing changes within the armed forces.

• There is a mismatch between acquiring modern technology and strengthening technological capability on the one hand, and the skills and structure of the armed forces on the other.

• A modern military depends on the defence industry, including the local defence industry, where resource availability and supply chains are crucial. Yet the strategy does not propose how the defence industry should develop, instead assuming that the market will determine progress or need. Such strategic industries require state attention, whereas other sectors relevant to the armed forces, such as textiles, do not require similar support because they also serve or could serve civilian purposes. Additionally, wartime-critical industries must be systematically maintained and developed, tested, kept minimally staffed and have their products continuously updated.

TABLE 2. CHANGES IN DEFENCE OBJECTIVES IN BRAZIL'S DEFENCE STRATEGIES, 1996–2016 (ADAPTED FROM MARQUES & MAIA NETO, 2020, PP. 18–19)

1996	2005	2012	2016
Guarantee sovereignty, preserve territorial integrity, heritage, and interests	Guarantee sovereignty, preserve national treasures and territorial integrity	Guarantee sovereignty, preserve national treasures and territorial integrity	Guarantee sovereignty, preserve national treasures and territorial integrity
Guarantee rule of law and democratic institutions			
Maintain national cohesion and unity	Contribute to the preservation of cohesion and national unity	Contribute to the preservation of cohesion and national unity	Contribute to the preservation of cohesion and national unity
	Promote regional stability	Contribute to regional stability	Contribute to regional stability, international peace and security
Contribute to maintaining international peace and security	Contribute to maintaining peace and international security	Contribute to international peace and security	
Protect individuals, goods, and resources that are Brazilian/under Brazilian jurisdiction	Defend national interests, Brazilian citizens' assets and resources abroad	Defend national interests, Brazilian citizens' assets and resources abroad	Protect individuals, goods, resources and national interests abroad
Achieve and maintain Brazilian interests abroad			
Give Brazil a significant role in international affairs and a greater role in international decision-making processes	Participation of Brazil in the community of nations and a broader role in international decision-making processes	Intensify Brazil's participation in the community of nations and international decisions	Increase Brazil's participation in the community of nations and role in international decision-making processes
		Maintain Armed Forces that are modern, joint, well-trained, balanced, professional and adequately deployed throughout the national territory	Assure the capability of defence for the accomplishment of the Armed Forces' constitutional missions
		Structure Armed Forces around capabilities, provide personnel and material in accordance with strategic and operational planning	

1996	2005	2012	2016
		Develop the Defence Industrial Base to ensure autonomy in vital technologies	Promote productive and technological autonomy in the area of defence
		Develop the potential for defence logistics and national mobilisation	
		Raise awareness amongst Brazilian people about the importance of defence matters for the country	Expand involvement of Brazilian society in National Defence matters

Recommendations for Estonia based on Brazil's example:

- Harmonise the activities of the defence industry with national defence needs. Even in innovation-driven Estonia, there are many start-ups and small companies developing modern military technology, but it would be useful to map where they are meeting Estonia's defence needs and where they are primarily serving commercial aims, so that the state can support missing competencies and industrial capacity as necessary.

- Align infrastructure development with national defence needs. Estonia would also benefit from coordinating national and societal infrastructure requirements with defence needs to avoid situations where infrastructure essential for societal continuity becomes a security risk.

- Amend legislation to ensure that the armed forces have not only the legal basis to support internal security functions during crises, but also the relevant training for internal security tasks.

Mexico

Mexico has compulsory one-year military service for all men aged 18–40, although conscripts are selected by lottery, and the service itself involves minimal training and is largely made up of social work. Conscripts serve only in the infantry. The Mexican Armed Forces (*Fuerzas Armadas de México*) are a professional military and consist of the army, navy and air force. Women are able to serve in the armed forces.

Mexico faces severe problems with drug cartels, organised crime and smuggling, which have led security and law-enforcement agencies to adopt increasingly hard-line and militarised approaches. The government has relied heavily on the armed forces (the *sustained militarisation of public security*), resulting in abuses of power and civilian deaths. Public safety and freedom of expression have become increasingly at risk. At the same time, defence spending has risen significantly as military responsibilities have expanded.

In Mexico, military information is classified, meaning legislators have no access to it. Both internal security and national security responsibilities are increasingly handed to the armed forces, leaving legislators ever more excluded from decision-making on security matters. The military now plays a growing role in the supervision of ports, border crossings and major infrastructure projects. This has raised further concerns about whether civilian authorities retain sufficient oversight of the military sector.

IN SEVERAL COUNTRIES, DOMESTIC INSTABILITY HAS LED TO THE MILITARY BEING AUTHORISED TO SUPPORT THE POLICE IN MAINTAINING PUBLIC SECURITY, OR EVEN TO ASSUME THAT ROLE OUTRIGHT. PHOTO: PEXELS.COM

This expansion of military responsibilities has also led to human rights abuses. The federal police has been replaced by the National Guard, which now serves as the main law-enforcement body. Private military and security companies also play an increasing role in maintaining national security.

Because the military is the primary driver of Mexico's internal security crisis, defence expenditure has risen significantly and arms imports grew by 17% between 2015 and 2019 (Transparency International Defence and Security, 2020f).

The *National Security Strategy* is a framework document covering a presidential term of office. It primarily defines the role and tasks of the military and the Ministry of Defence. The current strategy is the *National Peace and Security Plan 2018–2024* (*Plan Nacional de Paz y Seguridad 2018–2024*). However, a new strategy is expected soon following the election of a new president (Felbab-Brown, 2019).

The current plan identifies the following necessary measures (López Obrador, 2018), which, since the security strategy concerns regulations needed for society's safe and sustainable functioning, can also be seen as relevant to comprehensive national defence:

- The creation of a National Guard (comprising military police, naval police and soldiers), which will enable the military to carry out security and internal security activities (responsible authority: the Secretariat of Defence);
- Eliminating corruption and restoring the justice system;
- Ensuring employment, education, healthcare and welfare;

- Respecting and promoting human rights;

- The ethical regeneration of society;

- Fostering peace and relaunching the fight against illegal drugs;

- Recovery and dignity;

- Formulating a plan for internal security.

> **Recommendations for Estonia based on Mexico's example:**
>
> - Highlight the importance in the context of national defence of improving social welfare and living standards, that is, emphasise the significance of domestic stability as a part of national defence.
>
> - Prepare a plan for ensuring internal security as a part of national defence (e.g., an internal security development plan) with the aim of the strategic harmonisation of state and societal security.

Argentina

Argentina, South America's second-largest country, is politically relatively stable, which also means that the role of the military differs from that of other countries in the region (such as Brazil and Mexico). The military is fully professional, and compulsory military service was suspended in 1995. The President of Argentina is the commander-in-chief of the armed forces (*Fuerzas Armadas de la República Argentina*).

The country's current defence strategy, *National Defense (Decree 571/2020)*, states that, to address security issues, it is necessary to understand that internal security and national security are fundamentally separate (Defensa Nacional, 2020), and firmly stresses that this distinction must not be overlooked. In other words, Argentina's approach can be seen as the opposite of a comprehensive defence model, as societal resilience and state sovereignty are treated as distinct from one another.

Argentina's national defence focuses, in line with UN principles, on protecting the state against external aggression and aggressors. At the same time, *sub-regional defence systems* are no longer expected to require military support, and the military must not be assigned tasks other than national defence, including support to external missions.

Argentina's approach can be seen as the opposite of a comprehensive defence model, as societal resilience and state sovereignty are treated as distinct from one another.

In addition, the 2021 national defence directive *Poder Ejecutivo Nacional* stipulates that internal security is responsible for preventing, countering and investigating criminal threats, while the military's role in ensuring national security is limited to preventing and repelling military threats.

The Joint Chiefs of Staff are responsible for military cooperation and unit readiness, meaning that the army, navy and air force must all maintain continuity and training to fulfil their assigned duties. All state institutions must, however, be capable of handling "new threats" independently, requiring them to be organised and prepared in ways that do not rely on military assistance.

Suggestions for Estonia based on Argentina's example:

- Consider the principle of separating internal security and national defence, with a clear division in the defence strategy between internal security's role in preventing criminal threats and national defence's responsibility for external threats. Such a division helps ensure that resources are not tied up with tasks outside their mandate.

- Ensure general societal preparedness, both in the private sector and within internal security institutions, to strengthen the ability to cope independently and avoid relying on military support when facing "new threats".

2. QUANTITATIVE ANALYSIS OF NATIONAL DEFENCE STRATEGIES: ANALYSIS OF CHARACTERISTICS OF THE COUNTRIES INCLUDED IN THE STUDY

A quantitative analysis was carried out to assess the characteristics of the countries, considering the following factors:

- The existence of a comprehensive national defence strategy (yes–no)
- European Union membership (yes–no)
- NATO membership (yes–no)
- OECD membership (yes–no)
- System of government according to the democracy index
- Level of development
- Military capability

According to the 2023 Democracy Index, collated by The Economist Intelligence Unit, 19 of the 35 countries analysed have a comprehensive national defence system: 12 are categorised as *full democracies*, 6 as *flawed democracies*, and 1 as an authoritarian state (Figure 4).[4]

---

[4] As per the full results of the index, there are 24 full democracies, including Norway, New Zealand, Iceland, Sweden and Finland; 50 flawed democracies, including the United States, India and Brazil; 34 hybrid regimes, including Bangladesh, Ukraine and Nigeria; and 59 authoritarian regimes, including Saudi Arabia, as well as the Russian Federation and the People's Republic of China (The Economist Group, 2024).

TABLE 3. RELATIONSHIP BETWEEN THE PRESENCE OF COMPREHENSIVE NATIONAL DEFENCE AND SYSTEMS OF GOVERNMENT, 2023 (COMPILED BY THE AUTHORS)

		Countries with comprehensive national defence (number)	Countries without comprehensive national defence (number)
System of government according to the Democracy Index	Democracy	5	12
	Flawed democracy	7	6
	Hybrid regime	2	0
	Authoritarian	2	1

To present a consolidated overview of the countries, the characteristics of the 35 countries have been compiled into a table and the countries have been analysed according to certain characteristics (NATO, EU, democracy, military capability, etc.).

The study sample included 25 OECD countries, of which 15 have a comprehensive defence strategy, and 10 do not. Of the 10 countries in the sample that are not members of the OECD, only 4 have a comprehensive strategy.

FIGURE 3. EXISTENCE OF A COMPREHENSIVE NATIONAL DEFENCE PLAN IN 2024 BY OECD (LEFT) AND NATO (RIGHT) MEMBERSHIP (N=35) (ANALYSIS BY THE AUTHORS USING SPSS)
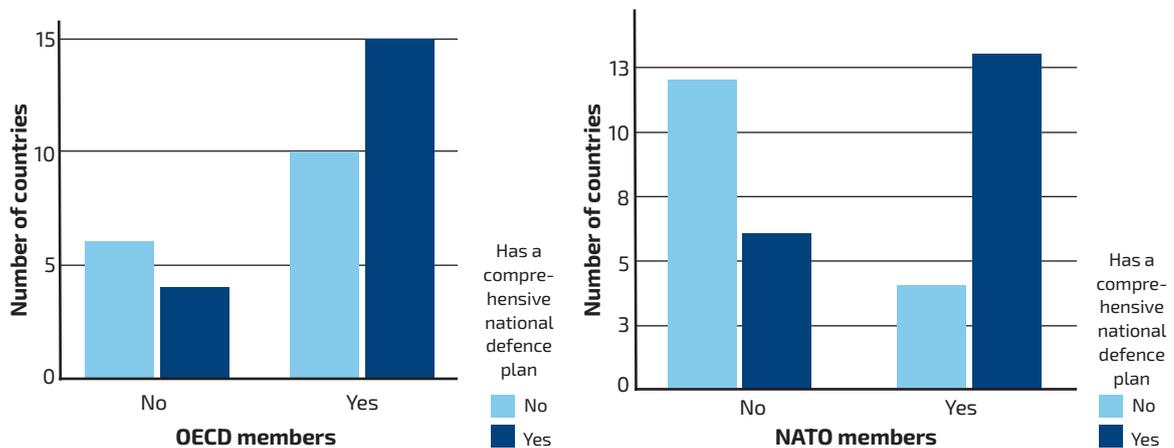
Of the 35 countries assessed, 17 are NATO members, 13 of which have a comprehensive national defence strategy. Among non-NATO states, the pattern is reversed, with 6 states having such a strategy and 13 without one.

FIGURE 4. DENDROGRAM OF COUNTRIES BY SIMILARITY (NATO, EU, OECD, GLOBAL NORTH–SOUTH, MILITARY STRENGTH, DEMOCRACY, LEVEL OF DEVELOPMENT) (COMPILED BY THE AUTHORS)
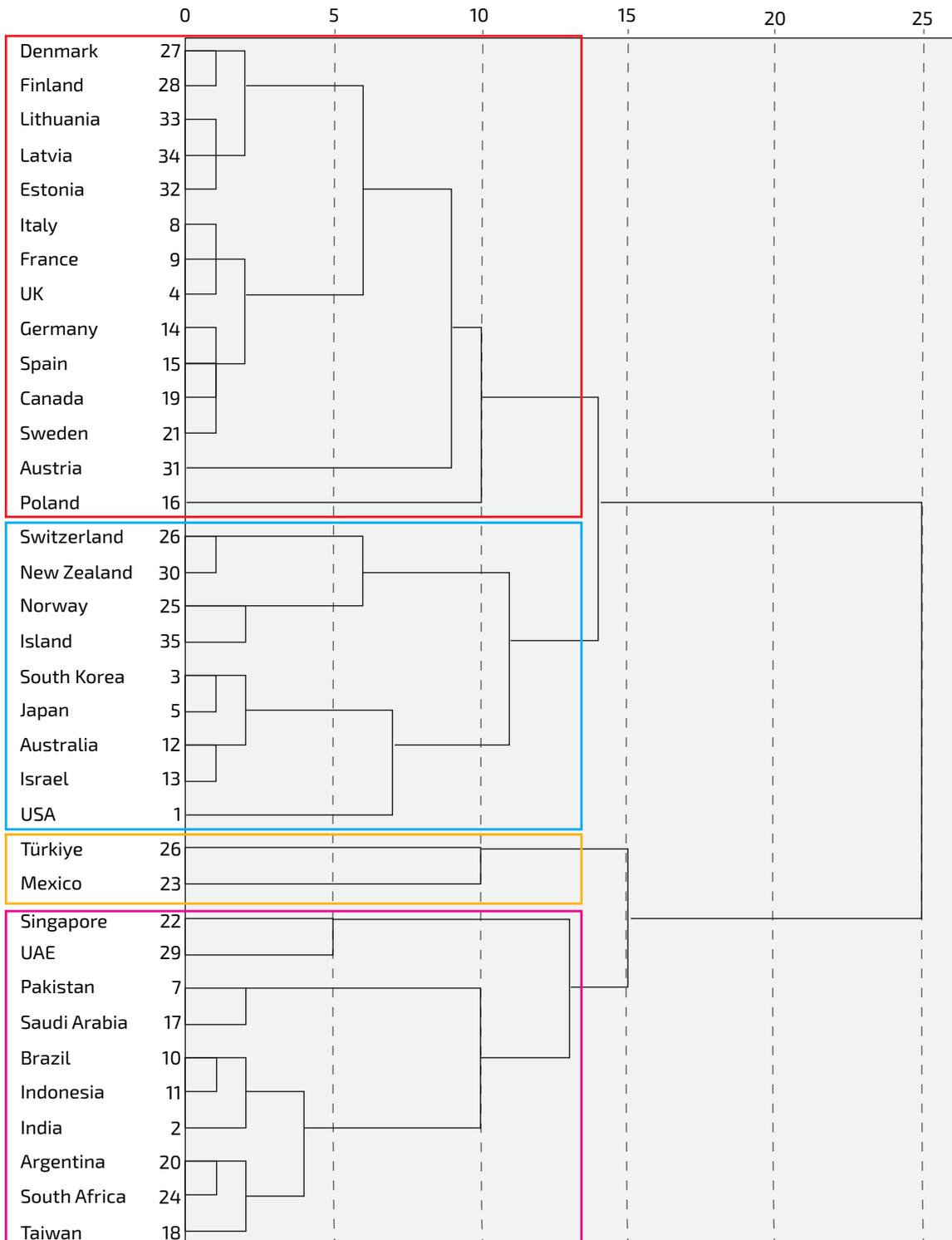
The dendrogram groups Estonia together with other countries according to their mutual similarity, using *Average Group Linkage* to form clusters. Estonia's first cluster is with the Baltic states, Denmark and Finland.

The next level of similarity links Estonia to Italy, France and the United Kingdom, and then to Germany, Italy, Canada and Sweden. These clusters show that Estonia shares

similarities with these countries on the NATO, EU and OECD membership, and military strength variables, democracy and level of development. Because the characteristics are measured on different scales (some on a 0–1 scale, democracy on a 0–10 scale, military strength on a 1–35 scale), they were all standardised as z-scores in advance to ensure that those with higher dispersion did not dominate the clustering; all variables thus have a variance of 1.

Across the national defence strategies reviewed – including the division of responsibilities within these strategies – the relationship between political authority and the military sector plays a central role:

- In European countries, national policy and the national armed forces are separate. This explains why the military's role is typically part of an integrated defence plan in which the field of internal security also has its own defined role and responsibilities.

- In the Latin American countries examined, the military is generally an extension of political power; military involvement in supporting domestic and foreign policy is therefore commonplace, and internal security is subordinated to central authority.

- In the Asian states examined, efforts have been made to separate powers – with varying degrees of success – and internal security is institutionally distinct, though it does not always have as clearly defined a role in national defence as in Europe.

- In North America, military capability also serves soft-power purposes by creating dominant dependency relationships with other states.

- In the Middle East, military capability likewise functions as a soft-power tool, although the principal focus is on developing the defence industry.

The concept of *total defence* is used in several countries, including Austria, Denmark, Finland, Indonesia, Lithuania, Norway, the Russian Federation, Singapore, Sweden, Serbia, Switzerland, Taiwan and Ukraine. This report covers Austria, Denmark, Finland, Lithuania, Norway, Singapore, Sweden, Switzerland and Taiwan. The meaning of the concept, however, differs across these contexts, generally falling into two categories: in the first, it denotes absolute military defence or defence readiness (as in Taiwan). In the second, it refers to comprehensive national defence in which national security is the outcome of the continuous and collective effort of the whole society.

In the context of the countries analysed, two distinct approaches to comprehensive or total defence can be identified:

- Total defence as a system in which all actors – institutions, enterprises and individuals – must support the armed forces as the highest defence authority. In this model, non-military sectors are expected to support defence objectives and to avoid creating additional burdens for the armed forces; for example, the military does not take responsibility for maintaining societal functioning during natural disasters or civil emergencies.

- Total defence as a system in which all sectors and the entire society are equal participants in national defence, each with its own role to fulfil.

It is also important, from the perspective of national crisis preparedness, to note that countries (particularly in Asia) that face extreme weather conditions – such as floods, hurricanes and earthquakes – explicitly incorporate such hazards, and their mitigation, into national defence planning. The same applies to food security and supply resilience.

CONCLUSIONS

The main recommendations for developing the internal security component of Estonia's comprehensive national defence derived from the preceding analysis are as follows.

- **Integration and co-operation:** Follow the examples of Finland, France and Spain by strengthening co-operation between ministries and local authorities, in addition to establishing a central coordination network or unit to enable fast and secure information exchange across the security system beyond the state sector. Strategic public and private enterprises should be involved in national defence and internal security planning.

- **Integration of internal security fields:** Drawing on the experience of Denmark and Norway, introduce a unified strategic framework that integrates the police and border guard, rescue services and other emergency services into a comprehensive national defence strategy. As in Poland, place greater attention on the role of medical and healthcare systems in security.

- **Societal resilience:** Based on Germany's principles of resilience, take a comprehensive approach to maintaining essential services, critical infrastructure and public order, including during emergencies. Improve the population's practical readiness for natural disasters and other hazards, following the examples of Switzerland, Indonesia and Singapore.

- **Cybersecurity and technology:** Run additional cybersecurity awareness and education programmes with as broad a range of target groups as possible, as in Austria. Create specialised intelligence units for detecting and neutralising cyber and biological threats, as in the UK.

- **Economic security and supply chains:** Emphasise the importance of economic security, as seen in South Korea, Pakistan and Taiwan, with a focus on safeguarding critical supply chains and domestic production capabilities.

- **Public engagement and education:** Promote societal awareness and understanding of national defence needs, drawing on the models of Taiwan and Singapore. Develop defence and security programmes for schools and communities.

- **Crisis preparedness:** Prioritise the further development of civil protection plans and the construction of civil protection facilities, following Switzerland and Brazil. Increase the role of local authorities in crisis preparedness, including managing local threats and involving residents and communities in practical preparedness activities.

- **International and regional co-operation:** Further promote close cooperation and experience-based knowledge exchange with neighbouring states and international partners to reinforce collective security, following Canada, Türkiye and the UAE.

- **Adaptation of the comprehensive defence concept:** Adopt the concept of comprehensive national defence across all societal domains, including in demilitarised form, with a focus on wider security principles, as reflected in Indonesia's approach.

- **Science and research:** Ensure that research and development is meaningfully involved in comprehensive national defence. This includes recognising the role of research in decision-making and in developing suitable security measures, as highlighted by Japan.

Based on the report, a set of sector-specific recommendations can be identified that are essential for developing the internal security component of Estonia's comprehensive national defence strategy. These should be elaborated in greater detail during strategy development, with careful attention to the specific security needs of the Estonian context. The recommendations fall into seven broad areas:

1. **Public engagement and awareness:** Introduce national programmes that involve all members of society and key stakeholder groups, following the example of Singapore. This includes educational programmes on civil protection and security (as in Norway). Develop child- and youth-focused educational initiatives and integrate security topics into curricula. Strengthen strategic communication as a component of national security strategy.

2. **Enhancing situational awareness:** Improve co-operation and operational capabilities across security agencies. This includes integrating the Defence Forces, the volunteer Estonian Defence League, the police and the emergency services into a unified situational awareness framework, following the Danish model. Reinforce information systems and data analytics to enable rapid and effective threat response. Apply scenario-based planning and scientific forecasting when preparing strategies, drawing on the examples of Denmark and Norway.

3. **Strengthening crisis preparedness and local authorities:** To improve crisis management and resource coordination at the local level, expand the role of local authorities in crisis management by providing additional resources and training. Civil protection solutions and community preparedness programmes should also be expanded. Apply similar practices to those in Norway and Switzerland for integrating crisis preparedness with local social and governmental structures, and emulate Finland's approach to cooperation between local authorities, communities, educational institutions, the private sector and NGOs. Increase the resources and capacity of the border guard reserve (as in Finland) and consider establishing a permanent crisis management staff modelled on France's example that would bring together representatives of different ministries and operate not only in the event of a crisis.

4. **Developing defence industry and technological capab**ility: Aim to modernise defence and security technologies, including autonomous systems. Invest in the domestic defence industry and potentially revise the defence procurement system, following the Canadian example. Promote technological innovation and develop links between the private sector and national security needs. Establish a programme for research and the development of security-relevant technologies, drawing on experience from Japan and Austria.

5. **Strengthening civil protection:** Increase participation across different target groups in civil protection and crisis preparedness training. Enhance public awareness of disinformation and hybrid threats, building on the experience of Lithuania and Poland. Expand the alternative or civilian service system, including increasing involvement in critical areas such as rescue services, social care and healthcare. This would also ensure preparedness to support these sectors during crises.

6. **International co-operation and collective defence:** Deepen co-operation with NATO and other international partners, with a focus on the dimensions of collective defence. Clarify Estonia's responsibilities in civil–military cooperation across different crisis scenarios down to the local government level, and maintain up-to-date knowledge of civil–military arrangements and capabilities in other European countries to ensure realistic planning for large-scale (regional or Europe-wide) crises.

7. **Investment and strategic planning:** Ensure adequate funding and support for security activities and strategic management. Increase the budget for defence and security tasks, publish national security strategies on a regular basis, conduct systematic analyses and launch a wide-ranging national defence education initiative to build awareness and skills across all population groups.

Based on the analysis presented in this report, it is clear that Estonia's national defence strategy should be comprehensive and inclusive and draw on international best practice. Particular emphasis should be placed on:

- Involving society as a whole and strengthening public understanding of security issues.

- Enhancing the role of local authorities in crisis management and civil protection.

- Developing science, technology and the defence industry.

- Improving situational awareness and expanding international co-operation.

The recommendations presented in this study will support the development of an internal security component for Estonia's comprehensive national defence that is coherent, integrated and geared towards strengthening resilience and involving all members of society.

REFERENCES

Amidror, Y., 2021. Israel's National Security Doctrine. *The Jerusalem Institute for Strategy and Security*, 18.07.2021. [Online] Available at: https://jiss.org.il/en/amidror-israels-national-security-doctrine/ [Accessed 16.01.2025].

Aoki, N., Tay, M., & Rawat, S., 2023. Whole-of-government and joined-up government: A systematic literature review. *Public Administration*, 102(2), pp. 733–752.

Australian Government Department of Defence, 2024a. *Integrated Investment Program 2024*. Canberra: Australian Government. [Online] Available at: https://www.defence.gov.au/about/strategic-planning/2024-national-defence-strategy-2024-integrated-investment-program [Accessed 17.01.2025].

Australian Government Department of Defence, 2024b. *National Defence Strategy 2024*. Canberra: Australian Government. [Online] Available at: https://www.defence.gov.au/about/strategic-planning/2024-national-defence-strategy-2024-integrated-investment-program [Accessed 17.01.2025].

Australian Government Department of Defence, 2023. National Defence: Defence Strategic Review 2023. Canberra: Australian Government. [Online] Available at: https://www.defence.gov.au/about/reviews-inquiries/defence-strategic-review [Accessed 17.01.2025].

Bankauskaité, D. & Šlekys, D., 2023. Lithuania's Total Defense Review. *PRISM*, 10(2), pp. 54–77.

Bērziņš, J., 2023. Latvia: From Total Defense to Comprehensive Defense. *PRISM*, 10(2), pp. 38–53.

Bozkurt, A., 2022. Turkey's 'secret constitution' may have defined the West as a major threat. *Nordic Monitor*, 28.03.2022. [Online] Available at: https://nordicmonitor.com/2022/03/turkeys-revised-secret-constitution-may-have-defined-nato-and-eu-as-a-major-threat/ [Accessed 16.01.2025].

Bundeskanzleramt, 2024. *Österreichische Sicherheitsstrategie*. Wien: Digitalprintcenter des BMI. [Online] Available at: https://www.bmlv.gv.at/download_archiv/pdfs/sicherheitsstrategie_oesterreich_2024.pdf [Accessed 16.01.2025].

Bundesministerium der Verteidigung, 2016. *Weißbuch zur Sicherheitspolitik und zur Zukunft der Bundeswehr*. Paderborn: Bonifatius GmbH. [Online] Available at: https://www.publikationen-bundesregierung.de/resource/blob/2277952/736102/90300c7ac5f41d817db77464ec7fe8a6/weissbuch-zur-sicherheitspolitik-2016-download-bmvg-data.pdf?download=1 [Accessed 16.01.2025].

Congressional Research Service, 2021. *The National Security Council: Background and Issues for Congress.* [Online] Available at: https://crsreports.congress.gov/product/pdf/R/R44828 [Accessed 03.11.2024].

Consiglio federale svizzero, 2021. *La politica di sicurezza della Svizzera: Rapporto del Consiglio federale.* Bern: Confederazione Svizzera. [Online] Available at: https://www.newsd.admin.ch/newsd/message/attachments/66393.pdf [Accessed 16.01.2025].

Danish Ministry of Defence, 2023. *Will and ability to take responsibility. Danish Defence Agreement 2024-2033.* [Online] Available at: https://www.fmn.dk/globalassets/fmn/dokumenter/forlig/-danish-defence-agreement-2024-2033-.pdf [Accessed 16.01.2025].

Defence Ministry of the Republic of Indonesia, 2016. *Defence white paper 2015.* [Online] Available at: https://www.kemhan.go.id/wp-content/uploads/2016/05/2015-INDONESIA-DEFENCE-WHITE-PAPER-ENGLISH-VERSION.pdf [Accessed 03.11.2024].

Defensa Nacional (2020) 26.06.2020. [Online] Available at: https://www.argentina.gob.ar/normativa/nacional/decreto-571-2020-339322 [Accessed 03.11.2024].

Department of National Defence, 2024. *Our North, Strong and Free: A Renewed Vision for Canada's Defence.* Ottawa: Department of National Defence. [Online] Available at: https://www.canada.ca/en/department-national-defence/corporate/reports-publications/north-strong-free-2024.html [Accessed 20.09. 2024].

Department of National Defence, 2017. *Strong, Secure, Engaged: Canada's Defence Policy.* [Online] Available at: https://www.canada.ca/en/department-national-defence/corporate/reports-publications/canada-defence-policy.html [Accessed 17.01.2025].

Dowse, A., 2024. Australia's Defense Strategy. *Journal of Indo-Pacific Affair*s, September-October. [Online] Available at: https://www.airuniversity.af.edu/JIPA/Display/Article/3900034/australias-defense-strategy/ [Accessed 16.01.2025].

Eesti Vabariigi Valitsus, 2023. *Eesti julgeolekupoliitika alused.* [Online] Available at: https://valitsus.ee/sites/default/files/documents/2023-03/eesti_julgeolekupoliitika_alused_est_22.02.pdf [Accessed 25.11.2024]

Felbab-Brown, V., 2019. *Amlo's security policy: creative ideas, tough reality.* The Brookings Institution. [Online] Available at: https://www.brookings.edu/wp-content/uploads/2019/03/FP_20190325_mexico_anti-crime.pdf [Accessed 16.01.2025].

Fremer, I., 2023. *Latvia: New Law Introduces Compulsory Military Service Starting in January 2024.* [Online] Available at: https://www.loc.gov/item/global-legal-monitor/2023-10-04/latvia-new-law-introduces-compulsory-military-service-starting-in-january-2024/ [Accessed 16.01.2025].

Goldwater-Nichols Department of Defense Reorganization Act of 1986 (1986) Public Law 99-433 (H.R. 3622), 04.10.1986. [Online] Available at: https://history.defense.gov/portals/70/documents/dod_reforms/goldwater-nicholsdodreordact1986.pdf [Accessed 19.12.2024].

Government of Iceland, 2023. *Parliamentary Resolution on a national security policy for Iceland. Resolution.* Parliamentary document 1231, item 487, no. 7/153 [Online] Available at: https://www.government.is/library/04-Legislation/Parliamentary%20

resolution%20on%20a%20national%20security%20policy%202023.pdf [Accessed 17.01.2025].

Government of Iceland, 2016. *National Security Council Act. Määrus.* Nr 98, 20.09.2016. [Online] Available at: https://www.government.is/publications/ legislation/lex/2018/01/19/National-Security-Council-Act-No.-98-20- September-2016/ [Accessed 17.01.2025].

Government of Iceland, [*s.a.*]a. Foreign Affairs. *Government of Iceland.* [Online] Available at: https://www.government.is/topics/foreign-affairs/national-security/ [Accessed 16.01.2025].

Government of Iceland, [*s.a.*]b. National Security. *Government of Iceland.* [Online] Available at: https://www.government.is/topics/public-safety-and-security/national-security/ [Accessed 16.01.2025].

Government of Singapore, [*s.a.*]. Total Defence: Together we Keep Singapore Strong. [Online] Available at: https://www.totaldefence.gov.sg/about/what-is-total-defence/ [Accessed 17.01.2025].

Government of South Africa, 1996. *National Defence White Paper.* [Online] Available at: https://www.gov.za/documents/white-papers/national-defence-white-paper-01-may-1996 [Accessed 17.01.2025].

Government Offices of Sweden, [*s.a.*]a. *Defence Resolution 2025-2030.* [Online] Available at: https://www.government.se/government-policy/total-defence/defence-resolution-2025-20302/ [Accessed 05.06.2025].

Government Offices of Sweden, [*s.a.*]b. *This is civil defence.* [Online] Available at: https://www.government.se/government-policy/civil-defence/this-is-civil-defence/ [Accessed 05.06.2025].

Hoetjes, G., 2022. *The Saudi-Emirati axis and the preservation of regional order.* Hauge: The Clingendael Institute. [Online] Available at: https://www.clingendael.org/sites/ default/files/2022-01/the-saudi-emirati-axis-and-regional-order.pdf [Accessed 17.01.2025].

Holmes, K. R., 2019. What is National Security? *The Heritage Foundation,* 07.10.2014. [Online] Available at: https://www.heritage.org/sites/default/files/2019-10/2015_ IndexOfUSMilitaryStrength_What%20Is%20National%20Security.pdf [Accessed 17.01.2025].

HM Government, 2015. *National security strategy and strategic defence and security review 2015: a secure and prosperous United Kingdom.* London: HM Government. [Online] Available at: https://assets.publishing.service.gov.uk/ media/5a74c796ed915d502d6caefc/52309_Cm_9161_NSS_SD_Review_web_only.pdf [Accessed 16.01.2025].

Il Ministro della Difesa, 2015. *Libro bianco per la sicurezza internazionale e la difesa.* Roma: Il Ministro della Difesa. [Online] Available at: https://www.analisidifesa.it/ wp-content/uploads/2015/04/Libro-Bianco-2015.pdf [Accessed 16.01.2025].

Jiang, H., 2020. The Logic of the Strategic Thinking and Defensive Measures of the Overall Defensive Concept of Taiwan. *Defense Security Brief,* 22.12. 2020. [Online] Available at: https://indsr.org.tw/en/respublicationcon?uid=15&resid=45&pid=1305 [Accessed 17.01.2025].

Jiwa Muda Indonesia, 2024. Strengthening National Defense: Defense Achievement Factors in the *2025-2045 RPJPN. Jiwa Muda Indonesia*, 3.07.2024. [Online] Available at:https://www.jiwamudaindo.com/strengthening-national-defense-defense-achievement-factors-in-the-2025-2045-rpjpn/ [Accessed 14.01.2025].

Kaitseministeerium, 2024. Laiapindne riigikaitse. [Online] Available at: https://kaitseministeerium.ee/et/eesmargid-tegevused/laiapindne-riigikaitse [Accessed 25.11.2024]

Kingdom of Saudi Arabia, 2016. *Saudi vision 2030*. [Online] Available at: https://www.vision2030.gov.sa/media/rc0b5oy1/saudi_vision203.pdf [Accessed 14.01.2025].

Koort, E., Loik, R., Puusalu, J. ja Savimaa, R., 2023. *Asendusteenistuse rakendamine Eesti kaitse- ja kriisivõimekuse eesmärkidesse.* Tallinn: Sisekaitseakadeemia. [Online] Available at: https://digiriiul.sisekaitse.ee/bitstream/handle/123456789/2968/Asendusteenistus-web.pdf?sequence=3 [Accessed 14.01.2025].

Koshino, Y., 2022. Japan's transformational national-security documents. *IISS*, 21.12.2022. [Online] Available at: https://www.iiss.org/online-analysis/online-analysis/2022/12/japans-transformational-national-security-documents/#:~:text=In%20releasing%20three%20historic%20strategy%20documents%20in%20December%2C,divide%20that%20has%20long%20undermined%20its%20defence%20sector [Accessed 04.12.2024].

Latvijas Republikas Aizsardzības ministrija, 2023. *The State Defence Concept 2023-2027*. [Online] Available at: https://www.mod.gov.lv/sites/mod/files/document/The%20State%20Defence%20Concept%202023-2027.pdf [Accessed 20.01.2025].

Latvijas Republikas Aizsardzības ministrija, [*s.a.*]a. *Comprehensive National Defence in Latvia*. [Online] Available at: https://www.mod.gov.lv/sites/mod/files/document/Comprehensive%20National%20Defence%20in%20Latvia.docx [Accessed 16.01.2025].

Latvijas Republikas Aizsardzības ministrija, [*s.a.*]b. *Comprehensive State Defence*. [Online] Available at: https://www.mod.gov.lv/en/nozares-politika/comprehensive-state-defence [Accessed 16.01.2025].

Lee, H-M., 2021. *Taiwan's Overall Defense Concept: Theory and the Practice.* [Online] Available at: https://www.hoover.org/sites/default/files/210927_adm_lee_hoover_remarks_draft4.pdf [Accessed 20.01.2025].

Lee, P. K., 2023. Seoul's new national security strategy flips the script, Korean style. *ASPI: The Strategist*, 13.06.2023. [Online] Available at: https://www.aspistrategist.org.au/seouls-new-national-security-strategy-flips-the-script-korean-style/ [Accessed 04.12.2024].

Lendon, B., 2023. South Korea sets nationwide civil defense drill, citing North's 'provocations. *CNN World*, 4.08.2023. [Online] Available at: https://edition.cnn.com/2023/08/04/asia/south-korea-civil-defense-drill-intl-hnk/index.html [Accessed 04.12.2024].

López Obrador, A. M., 2018. *Plan nacional de play y seguridad 2018-2024.* [Online] Available at: https://lopezobrador.org.mx/wp-content/uploads/2018/11/Plan-Nacional-de-Paz-y-Seguridad_.pdf

Manar Military Company [MMC], 2024. UAE's evolving defense strategy in a changing world. [Online] Available at: https://www.mmc.ae.org/articles/uae-s-evolving-defense-strategy-in-a-changing-world [Accessed 04.12.2024].

Marek, A., 2020. Heimevernet – the Pillar of Norway's Defence Policy. *War Studies University Scientific Quarterly,* 3(116), pp.103–118.

Marques, A. A. & Maia Neto, J., 2020. Brazil's National Defence Strategy, Defence Diplomacy and Management of Strategic Resources. Rmt: I. Liebenberg, D. Kruijt & S. Paranjpe, toim-d. *Defence Diplomacy and National Security Strategy.* Stellenbosch: African Sun Media, pp. 13–32.

Matthews, R. & Bintang Timur, F., 2023. Singapore's 'Total Defence' Strategy. *Defence and Peace Economics*, 35(5), pp. 638–658.

Meridor, D. & Eldadi, R., 2019. *Israel's National Security Doctrine: The Report of the Committee on the Formulation of the National Security Doctrine (Meridor Committee), Ten Years Later.* Tel Aviv: The Institute for National Security Studies (INSS). [Online] Available at: https://www.inss.org.il/wp-content/uploads/2019/02/Memo187_11.pdf [Accessed 04.12.2024].

Ministry of Defence, 2024. *New total defence resolution for a stronger Sweden.* Government Offices of Sweden, 15.10.2024. [Online] Available at: https://www.government.se/press-releases/2024/10/new-total-defence-resolution-for-a-stronger-sweden/ [Accessed 05.06.2025].

Ministerio de Defensa de España, 2021. *Estrategia de Seguridad Nacional.* Madrid: Publicaciones oficiales de la AGE. [Online] Available at: https://www.dsn.gob.es/sites/default/files/documents/ESN2021%20Accesible_1.pdf [Accessed 16.01.2025].

Ministère de la Défense, 2013. *Livre blanc; défense et sécurité nationale; 2013.* Paris: Direction de l'information légale et administrative. [Online] Available at: https://ccdcoe.org/uploads/2018/10/Livre-blanc-sur-la-Defense-et-la-Securite-nationale-2013-2.pdf [Accessed 16.01.2025].

Ministry of National Defense, 2023. *ROC National Defense Report 2023.* Online] Available at: https://www.mnd.gov.tw/newupload/ndr/112/112ndreng.pdf [Accessed 04.12.2024].

Ministry of National Defence, 2022. *Defence White Paper, 2022.* [Online] Available at: https://www.mnd.go.kr/user/mndEN/upload/pblictn/PBLICTNEBOOK_202307280406019810.pdf [Accessed 04.12.2024].

Ministry of National Defence of the Republic of Lithuania, 2023. *Strategic provisions.* [Online] Available at: https://kam.lt/en/strategic-provisions/ [Accessed 17.01.2025].

Morwinsky, O., Clobes, A. & Šimaitytė, F., 2024. *Baltic Bastions: New defence strategies for Lithuania, Latvia and Estonia.* [Online] Available at: https://www.kas.de/en/country-reports/detail/-/content/new-defence-strategies-for-lithuania-latvia-and-estonia [Accessed 17.01.2025].

Muneer, S. & Aryal, S.K., 2024. *Cause and Effect: The Factors that Make Pakistan's Military a Political Force.* [Online] Available at: https://www.orfonline.org/research/cause-and-effect-the-factors-that-make-pakistans-military-a-political-force [Accessed 17.01.2025].

National Cybersecurity Authority, 2020. *Kingdom of Saudi Arabia National Cybersecurity Strategy (Overview).* [Online] Available at: https://cdn.nca.gov.sa/api/files/public/upload/b2bf9688-b7d1-4cd2-8e40-d075612a2323_national_cybersecurity_strategy-en.pdf [Accessed 17.01.2025].

National Defence Act (2012). The R.O.C laws & regulations database, 06.06.2012. [Online] Available at: https://law.moj.gov.tw/ENG/LawClass/LawAll. aspx?pcode=F0010030 [Accessed 04.12.2024].

National Security Bureau, 2020. *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*. Warszawa: National Security Bureau. [Online] Available at: https://www. bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf [Accessed 16.01.2025].

National Security Division, 2022. *National Security Policy of Pakistan 2022-2026*. [Online] Available at: https://dnd.com.pk/wp-content/uploads/2022/01/National-Security-Policy-2022-2026.pdf [Accessed 04.12.2024].

NATO Parliamentary Assembly, 2023. *Iceland's Comprehensive Approach to Security is Complemented by a National Focus on Harnessing Natural Resources and Innovation.* [Online] Available at: https://www.nato-pa.int/news/icelands-comprehensive-approach-security-complemented-national-focus-harnessing-natural [Accessed 17.01.2025].

New Zealand Government, 2023. *Secure Together. New Zealand's National Security Strategy 2023-2028*. [Online] Available at: https://www.dpmc.govt.nz/sites/default/files/2023-11/national-security-strategy-aug2023.pdf [Accessed 17.01.2025].

New Zealand Ministry of Defence, 2023a. *Defence Policy and Strategy Statement 2023*. [Online] Available at: https://www.defence.govt.nz/publications/defence-policy-review-defence-policy-and-strategy-statement-2023/ [Accessed 17.01.2025].

New Zealand Ministry of Defence, 2023b. *Future Force Design Principles 2023*. [Online] Available at: https://www.defence.govt.nz/publications/defence-policy-review-future-force-design-principles-2023/ [Accessed 17.01.2025].

New Zealand Defence Forces, 2019. *The NZDF Strategic Plan 2019–2025*. [Online] Available at: https://www.nzdf.mil.nz/assets/Uploads/DocumentLibrary/NZDF-Strategic-Plan-2019-2025-v2.pdf [Accessed 20.01.2025].

Ng, J. & Jasmine, S., 2021. *Indonesia's National Mobilisation Strategy: Growing Deeper Roots?* [Online] Available at: https://www.rsis.edu.sg/wp-content/uploads/2021/02/CO21023.pdf [Accessed 04.12.2024].

Norwegian Defence Research Establishment, [*s.a.*]. [Online] Available at: *Total Defence*. https://www.ffi.no/en/about-ffi/total-defence [Accessed 17.01.2025].

Norwegian Ministry of Defence, 2023a. *Future Acquisitions For the Norwegian Defence Sector 2023–2030*. [Online] Available at: https://www.regjeringen.no/contentassets/595f6354301a4d7b9d63ef1c8e486482/faf-2023-2030-engelsk-versjon. pdf [Accessed 16.01.2025].

Norwegian Ministry of Defence, 2023b. T*he Norwegian Defence Pledge. Long-term Defence Plan 2025–2036*. [Online] Available at: https://www.regjeringen.no/en/dokumenter/the-norwegian-defence-pledge/id3032809/?ch=1 [Accessed 16.01.2025].

Office of National Security, 2023. The Yoon Suk Yeol Administration's National Security Strategy (June 2023). [Online] Available at: https://overseas.mofa.go.kr/viewer/skin/doc.html?fn=20230621040037933.pdf&rs=/viewer/result/202412 [Accessed 04.12.2024].

Park, H. R., 2023. Yoon administration releases its National Security Strategy. [Online] Available at: https://www.mofa.go.kr/us-en/brd/m_4511/view.do?seq=761767 [Accessed 04.12.2024].

Poder Ejecutivo Nacional, 2021. *Directiva de política de defensa nacional. Decreto.* 457/2021 (DCTO-2021-457-APN-PTE). [Online] Available at: https://www.argentina.gob.ar/normativa/nacional/decreto-457-2021-352107/texto [Accessed 04.12.2024].

Política Nacional de Defesa (PND) (2013) 25.09.2013. [Online] Available at: https://www.gov.br/defesa/pt-br/arquivos/2012/mes07/pnd.pdf [Accessed 04.12.2024].

President of the Republic of Indonesia, 2021. *Kebijakan umum pertahanan negara tahun 2020–2024.* [Online] Available at: https://peraturan.bpk.go.id/Download/150427/Salinan%20Perpres%20Nomor%208%20Tahun%202021.pdf [Accessed 04.12.2024].

Randma-Liiv, T., & Sarapuu, K. 2019. Chapter 11: Public governance in small states: from paradoxes to research agenda. Rmt: Massey. A., toim. *A Research Agenda for Public Administration*. Cheltenham, UK: Edward Elgar Publishing. pp. 162–179.

Public Safety Canada, 2024. *National Security*. [Online] Available at: https://www.publicsafety.gc.ca/cnt/ntnl-scrt/index-en.aspx [Accessed 20.01.2025].

Republic of South Africa Defence Department, 2020. *Department of Defence strategic plan for 2020–2025.* [Online] Available at: https://www.parliament.gov.za/storage/app/media/Docs/tpap/5a2878b3-e7a0-4568-87d8-776234e41173.pdf [Accessed 04.12.2024].

Republic of Türkiye Ministry of Foreign Affairs, 2022a. I. Türkiye's Perspectives and Policies on Security Issues. [Online] Available at: https://www.mfa.gov.tr/i_-turkiye_s-security-perspective_-historical-and-conceptual-background_-turkiye_s-contributions.en.mfa [Accessed 04.12.2024].

Republic of Türkiye Ministry of Foreign Affairs, 2022b. National foreign policy in the „Century of Türkiye". [Online] Available at: https://www.mfa.gov.tr/synopsis-of-the-turkish-foreign-policy.en.mfa [Accessed 04.12.2024].

Reza, B. I., 2017. The total people's defense and security system: problems of the state-sponsored militia in Indonesia. *Indonesia Law Review*, 2(7), pp. 155-177.

Riopelle, M. W., 2022. *Formulating Canadian National Security Strategy: A Process to Create a Deliberate and Persistent Strategic Security Policy in Canada. Magistritöö.* Fort Leavenworth: U.S. Army Command and General Staff College. [Online] Available at: https://apps.dtic.mil/sti/citations/trecms/AD1210972 [Accessed 17.01.2025].

Saxi, H. L., 2023. Norway Between the „High North" and the Baltic Sea. *PRISM*, 10(2), pp. 112–129.

Shankar IAS Parliament, 2024. National Security Doctrine. *Shankar IAS Parliament*, 27.06.2024. [Online] Available at: https://www.shankariasparliament.com/current-affairs/national-security-doctrine [Accessed 04.12.2024].

Singapore Civil Defence Force, [s.a.]. *What is Total Defence.* [Online] Available at: https://www.scdf.gov.sg/home/community-volunteers/community-preparedness/total-defence [Accessed 04.12.2024].

Sisäministeriö, 2019. *Maailman turvallisinta maata tekemässä*. Helsinki: Sisäministeriö. [Online] Available at: https://julkaisut.valtioneuvosto.fi/bitstream/

handle/10024/161676/SM_27_19_Maailman%20turvallisinta%20maata%20
tekemassa.pdf [Accessed 16.01.2025].

Sisäministeriö, 2017. H*yvä elämä – turvallinen arki.* Helsinki: Sisäministeriö. [Online]
Available at: https://julkaisut.valtioneuvosto.fi/server/api/core/bitstreams/68825d-
cd-f30c-4e7e-ad9a-b9d297ffaa6c/content [Accessed 16.01.2025].

Sisäministeriö, 2016. *Valtioneuvoston selonteko sisäisestä turvallisuudesta.* Helsinki:
Lönnberg Print & Promo. [Online] Available at: https://intermin.fi/docu-
ments/1410869/4113506/67644_julkaisu_082016.pdf [Accessed 16.01.2025].

Siqueira Brick, E., 2020. *Sumário Executivo Análise crítica dos documentos de alto nível
da defesa do Brasil*. [Online] Available at: https://defesa.uff.br/wp-content/uploads/
sites/342/2020/11/Anlise-PND_END_LBDN_Sumrio-Executivo.pdf [Accessed
04.12.2024].

Stebbins, R. A., 2001. *Exploratory Research in the Social Sciences.* Thousand Oaks,
Calif.: Sage Publications.

Swedberg, R., 2020. Exploratory Research. Rmt: Elman, C., Gerring, J., & Mahoney,
J., toim-d. *The Production of Knowledge: Enhancing Progress in Social Science.*
Cambridge: Cambridge University Press, pp. 17–41.

Taiwan ICDF, 2023. Taiwan Youth Overseas Service. [Online] Available at: https://
www.icdf.org.tw/wSite/ct?xItem=5380&ctNode=31595&mp=2#:~:text=In%20
January%202000%2C%20the%20government,community%20service%2C%20and%20
environmental%20agencies [Accessed 04.12.2024].

Tank, P., 2021. Between Human and State Security: Turkey's Syria Policy under the
Justice and Development Party (AKP). *The International Spectator*, *56*(4), pp. 84–100.

The Economist Group, 2024. EIU's 2023 Democracy Index: conflict and polarisation
drive a new low for global democracy. *The Economist Group*, 15.02.2024. [Online]
Available at: https://www.economistgroup.com/press-centre/economist-intelligence/
eius-2023-democracy-index-conflict-and-polarisation-drive-a-new-low-for [Accessed
05.03.2025].

The Geneva Centre for the Democratic Control of Armed Forces [DCAF], 2011.
Police Legislation Model – Japan. [Online] Available at: https://www.dcaf.ch/sites/
default/files/publications/documents/Japan%20Police_Eng_13-10-11.pdf [Accessed
05.01.2025].

The Government of Japan, 2022a. *National Security Strategy of Japan 2022.* [Online]
Available at: https://www.cas.go.jp/jp/siryou/221216anzenhoshou/national_security_
strategy_2022_pamphlet-e.pdf [Accessed 04.12.2024].

The Government of Japan, 2022b. *Defense buildup program*. [Online] Available
at: https://www.mod.go.jp/j/policy/agenda/guideline/plan/pdf/program_en.pdf
[Accessed 04.12.2024].

The Security Policy Analysis Group, 2022. *Danish Security and Defence towards 2035*.
[Online] Available at: https://www.fmn.dk/globalassets/fmn/dokumenter/strategi/
rsa/-regeringens_security-policy-report_uk_web-.pdf [Accessed 16.01.2025].

The White House, 2022. *National Security Strategy.* [Online] Available at: https://
www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-
National-Security-Strategy-10.2022.pdf [Accessed 09.10.2024].

Theussen, A., 2023. Denmark's Security Starts in the Baltic States. *PRISM*, 10(2), pp. 166–181.

Thorhallsson, B. & Wivel, A., 2006. Small States in the European Union: What Do We Know and What Would We Like to Know? *Cambridge Review of International Affairs*, 19(4), pp. 651–668.

Tiimonen, H. & Nikander, M., 2016. *Sisäisen ja ulkoisen turvallisuuden keskinäisriippuvuus*. Helsinki: Sisäministeriö. [Online] Available at: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79229/Sisaisen_ja_ulkoisen_turvallisuuden_keskinaisriippuvuus.pdf?sequence=1 [Accessed 04.12.2024].

TotalDefenceSG, 2016. *There's a Part for Everyone Music Video*. 10. veebruar 2016. [Online] Available at: https://www.youtube.com/watch?v=jyXZyffn5e8 [Accessed 12.10.2024].

Total Military Insight, 2024. Military Influence on Politics in Pakistan: An In-Depth Analysis. *Total Military Insight*, 08.07.2024. [Online] Available at: https://totalmilitaryinsight.com/military-influence-on-politics-in-pakistan/ [Accessed 04.12.2024].

Transparency International Defence and Security, 2020a. *Government Defence Index. Country Brief: Indonesia*. [Online] Available at: https://ti-defence.org/wp-content/uploads/sites/3/2021/11/Indonesia_GDI-2020-Brief.pdf [Accessed 04.12.2024].

Transparency International Defence and Security, 2020b. *Government Defence Index. Country Brief: Saudi Arabia*. [Online] Available at: https://ti-defence.org/gdi/wp-content/uploads/sites/3/2021/11/Saudi-Arabia_GDI-2020-Brief.pdf [Accessed 04.12.2024].

Transparency International Defence and Security, 2020c. *Government Defence Index. Country Brief: United Arab Emirates*. [Online] Available at: https://ti-defence.org/gdi/wp-content/uploads/sites/3/2021/11/United-Arab-Emirates_GDI-2020-Brief.pdf [Accessed 04.12.2024].

Transparency International Defence and Security, 2020d. *Government Defence Index. Country Brief: South Africa*. [Online] Available at: https://ti-defence.org/gdi/wp-content/uploads/sites/3/2021/11/South-Africa_GDI-2020-Brief.pdf [Accessed 04.12.2024].

Transparency International Defence and Security, 2020e. *Government Defence Index. Country Brief: Brazil*. [Online] Available at:https://ti-defence.org/gdi/wp-content/uploads/sites/3/2021/11/Brazil_GDI-2020-Brief.pdf [Accessed 04.12.2024].

Transparency International Defence and Security, 2020f. *Government Defence Index. Country Brief: Mexico*. [Online] Available at: https://ti-defence.org/wp-content/uploads/sites/3/2021/11/Mexico_GDI-2020-Brief.pdf [Accessed 04.12.2024].

U.S. Department of Defense, 2022. *National Defense Strategy of the United States of America including the Nuclear Posture Review and the Missile Defense Review*. [Online] Available at: https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/NATIONAL-DEFENSE-STRATEGY-2022.PDF [Accessed 12.10.2024].

United Nations Educational, Scientific and Cultural Organization Main Title, 2023. Governance: A whole-of-society approach. *The United Nations World Water Development Report 2023,* pp. 172–182.

Wither, J. K., 2020. Back to the future? Nordic total defence concepts. *Defence Studies*, 20(1), pp. 61–81.

Wrange, J., Bengtsson, R., & Brommesson, D., 2024. Resilience through total defence: Towards a shared security culture in the Nordic-Baltic region? *European Journal of International Security*, 9(4), pp. 511–532.

Yanan, L., 2024. Turkish National Security Strategy: Evolution, Characteristics, and Practices. *CIR*, 34(3), pp. 52–78.

Yeşiltaş, M., 2020. Deciphering Turkey's Assertive Military and Defense Strategy: Objectives, Pillars, and Implications. *Insight Turkey*, 22(3), pp. 89–114.

Yong-sup, H., 2006. Analyzing South Korea's Defense Reform 2020. *Korean Journal of Defense Analysis*, 18(1), pp. 111–134.

ANNEX. TABLES AND FIGURES BASED ON THE ANALYSIS OF COUNTRIES

TABLE A1. COUNTRY CLASSIFICATION ON THE SO-CALLED NORTH–SOUTH SCALE (N=35) (COMPILED BY THE AUTHORS)

	Existence of a comprehensive defence strategy		Development level		Military capability (scale 1–35, 1 = weakest)
	No	Yes	Developed	Developing	Arithmetic mean
South (BRICS/CIS/SCO)	2	0	1	1	10
North (NATO/EU/MNNA/Quad/OECD)	10	16	22	4	17
Neither	4	3	1	6	25

TABLE A2. COUNTRY CLASSIFICATION BY THE EXISTENCE OF A COMPREHENSIVE DEFENCE STRATEGY (N=35) (COMPILED BY THE AUTHORS)

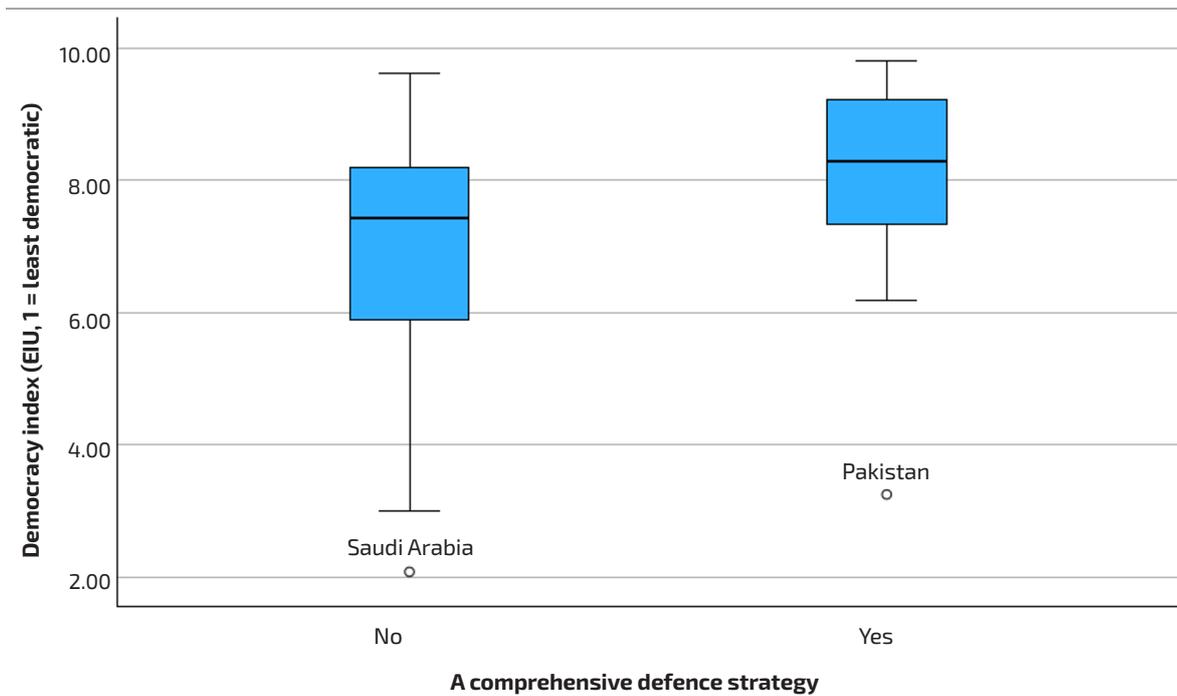|	NATO membership		EU membership		Military strength (scale 1–35, 1 = weakest)	Democracy Index (EIU) (1 = least democratic)
	No	Yes	No	Yes	Arithmetic mean	Arithmetic mean
Yes	6	13	8	11	15	8,05
No	12	4	13	3	21	6,79

FIGURE A1. RELATIONSHIP BETWEEN THE EXISTENCE OF A COMPREHENSIVE DEFENCE STRATEGY AND DEMOCRACY (BOXPLOT) (COMPILED BY THE AUTHORS)
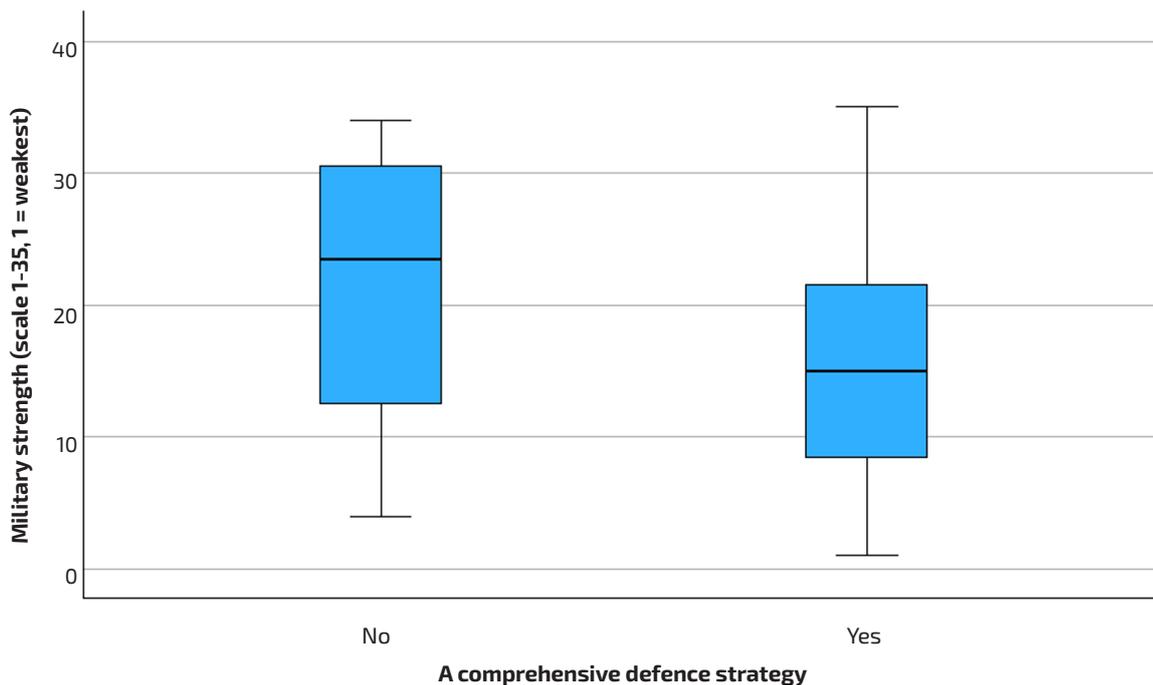

FIGURE A2. PRESENCE OF A COMPREHENSIVE NATIONAL DEFENCE STRATEGY AND MILITARY STRENGTH (BOXPLOT) (COMPILED BY THE AUTHORS)

THE RESEARCH REPORT EXAMINES COMPREHENSIVE NATIONAL DEFENCE STRATEGIES AND HOW THEY HAVE BEEN IMPLEMENTED IN THE FIELD OF INTERNAL SECURITY, FOCUSING ON THE ANALYSIS OF INTERNATIONAL EXPERIENCES AND THE IDENTIFICATION OF BEST PRACTICES.

This report describes a study that analysed the national defence strategies of 34 countries and the process of drafting those strategies. The report highlights both good practices and the complexities of this process, therefore providing evidence-based input for developing Estonia's comprehensive national defence strategy and the strategy-drafting process.

The aim of the report is to support a comprehensive approach to Estonia's national defence, which, in addition to military defence, also involves internal security, the public sector, private enterprises and civil society. The internal security component of this national defence approach should focus on ensuring societal stability and resilience and on preventing critical threats, including cyberattacks, the spread of disinformation, and hybrid threats.

The report emphasises that the success of a comprehensive national defence strategy depends on an integrated and synergistic approach that involves all levels of society. The lessons learned from international practices provide Estonia with an opportunity to shape an effective and resilient national defence system that can adapt to current and future security threats.