

Resilience Review Paper

Promoting Reform Objectives
through Technical Expertise and
Capacity Transfer.

Funded by Global Affairs
Canada. Implemented
by Alinea.



©2022 Alinea International. All rights reserved. Reproduction of the Review Paper in whole or in part is permitted provided that reference is made on Alinea International, and provided that such reproduction, in whole or in part, is without resale publication or inclusion of a portion of the reproduced text in a publication to be sold. Appropriate written permission from Alinea International must be obtained if the reproduction involves adaptation or modification of the original content.

Authors: experts of the PROTECT program (Promoting Reforms Objectives through Technical Expertise and Capacity Transfer), implemented by Alinea International in Ukraine as well as experts of the Government Office for Coordination of European and Euro-Atlantic Integration:

Victoria Vdovychenko, Team Lead, ANP-NATO Reform Initiative

Denys Chorny, Deputy Director, Government Office for Coordination of European and Euro-Atlantic Integration

Iryna Maistrenko, State Expert, Government Office for Coordination of European and Euro-Atlantic Integration

Dmytro Melnyk, M&E Expert, ANP-NATO Reform Initiative

Inna Potapova, State expert, Government Office for Coordination of European and Euro-Atlantic Integration

Igor Protsyk, Defence Expert, ANP-NATO Reform Initiative

Pavlo Sergaiev, Security Expert, ANP-NATO Reform Initiative

Oleksandr Tsarenok, Communications Expert, ANP-NATO Reform Initiative

Vladyslav Yasniuk, Policy Advisor, ANP-NATO Reform Initiative

Alinea International is not responsible for the consequences of using this information for other purposes or in another context. This publication was made possible due to the support of the Government of Canada at the request of the Government Office for Coordination of European and Euro-Atlantic Integration. The content of this publication should not be construed as reflecting the position of the Government of Canada.

Table of Contents

Table of Contents	3
Introduction	4
NATO	7
European Union	9
Resilience	9
Legislation	9
Four Dimensions of Resilience	10
Resilience dashboard	10
Conclusions	11
Bulgaria	12
Resilience	12
Legislation	12
Institutions	13
Conclusion	13
Estonia	14
Resilience	14
Legislation	14
Institutions	16
Conclusions	17
Finland	18
Resilience	18
Legislation	19
Institutions	20
Conclusions	27
Lithuania	28
Resilience	28
Legislation	28
Institutions	32
Conclusion	37
Latvia	38
Resilience	38

Legislation	38
Institutions	41
Conclusions	46
Poland	46
Resilience	46
Legislation	49
Institutions	50
Conclusions	53
Romania	54
Resilience	54
Legislation	55
Institutions	56
Conclusions	59
Israel	59
Resilience	59
Legislation	60
Institutions	60
Conclusion	64
United Kingdom	65
Resilience	65
Legislation	66
Institutions	68
Conclusions	69
General Conclusions	70
Recommendations	72
Appendix	74
Annex 1. Questionnaire for Experts	74
Annex 2. Logic Model	75
Annex 3. Extra Sources	77
Annex 4. Focus Group Experts	78

Introduction

The **National Security Strategy of Ukraine**, approved by the Decree of the President of Ukraine of September 14, 2020, № 392/2020, describes both a broad set of risks and threats, as well as national structural weaknesses. The **Concept of the National Resilience System**, approved by the Decree of the President of Ukraine of September 27, 2021, № 479/2021, defines the purpose, basic principles, directions, mechanisms and terms of implementation and functioning of the national sustainability system aimed at ensuring the ability of the state and society to identify threats, identify vulnerabilities and assess national security risks, their negative impacts, respond effectively and recover quickly and fully from emergencies or emergencies of all kinds, including but not limited to hybrid threats.

Implementation of the Concept will contribute to the implementation of the **national resilience system**; introduction of a **risk-oriented approach** in the system of strategic analysis and planning; ensuring the **appropriate level of readiness** of the state and society to respond to threats to national security, emergencies and crises of various origins at all stages; establishing **effective cooperation between all actors** in ensuring national stability; improving the **efficiency of crisis management** of the state; **reduction of human, material and financial losses** due to threats, crises of all kinds; **consolidation of society, increasing the level of trust in the government**; strengthening the **capacity of territorial communities**, development of local self-government in the context of preventing and counteracting threats, emergencies and crises; **saving resources** through their efficient use; and the development of **international cooperation and exchange of experience** in the field of building the national system of stability and integration of Ukraine into the Euro-Atlantic security system.

The **goal of this Resilience Review (hereunder- the Review)** is to collect the lessons from a set of countries and organizations that have relevant experience in resilience-building in order to support Ukraine to build its national resilience system better. It will help the Governmental Office on European and Euro-Atlantic Integration to make sure that Ukraine uses the cutting edge experience in resilience to strengthen Ukraine's democratic governance, reaffirm its value in addressing current and emerging security challenges as well as driving innovative responses to current and emerging security challenges imposed by the Russian full scale aggression of Ukraine.

The **objectives of this Review** are to: (a) better inform Ukrainian decision makers on how other countries advance their efforts in building both more robust and resilient systems as well as set preconditions for the resilient societies; (b) create incentives for more widespread and effective resilience adaptation through enhanced transparency; (c) identify best practices to allow proven lessons on resilience to be scaled up across sectors in Ukraine.

For the purpose of this Review we will use the terms of resilience as defined by the National Resilience System Concept, in particular:

- **national system of resilience** as a complex of purposeful actions, methods and mechanisms of interaction of state authorities, local self-government bodies, enterprises, institutions, organizations, civil society institutes that guarantee the preservation of safety and continuity of functioning of the main spheres of life of society and the state before, during and after the onset crisis situation;
- **national resilience** - as the ability of the state and society to effectively resist threats of any origin and nature, to adapt to changes in the security environment, to maintain stable functioning, to quickly recover to the desired balance after crisis situations;
- **organizational resilience** as the ability of state authorities, local self-government bodies, enterprises, institutions, organizations to identify, prepare, respond to threats, adapt to changes

in the security environment, maintain stable functioning before, during and after the onset of a crisis situation in order to maintain functioning and further development;

This Review aims to collect the experiences and best practices from a set of countries to support the **Implementation Plan of the Concept of ensuring the national system of resilience (Implementation Plan of the National Resilience System Concept)**. Diverse in geography, each of the chosen profiles presents a unique system of lessons identified and lessons learned for Ukraine representing EU/non-EU, NATO/non-NATO members. In particular, taking into account Ukraine's recently granted EU candidacy status, the focus of the Review will be on **Finland, Poland, Estonia, Latvia, Lithuania, Romania, Bulgaria** all of which geographically are close to Ukraine, and have a common historical legacy and understanding of the threat posed by the Russian Federation. At the same time, the majority of the selected countries are also NATO members. Among the non-EU members, the experience of the **UK and Israel** is believed to have special relevance because of their history and geostrategic situation.

The Review starts with an overview of how resilience is being understood by NATO and EU. Having declared full membership of Ukraine in the European Union and the North Atlantic Treaty Organization a strategic course of the state, it is equally important to identify their standards and expectations for resilience. From the other side, we would like to see how responsiveness of NATO itself was effective towards the threats imposed by the Russian full scale invasion of Ukraine. In this regard and as part of the methodology review, we've embedded 7 baselines of resilience approved by the Warsaw NATO summit.

At the same time, we see it as a trend that the new era of challenges foster EU and NATO vision resilience as 'one voice' policy. The recent establishment of a structured dialogue on resilience between EU and NATO will further strengthen interaction in this key work strand¹.

The Review continues with the country's profiles encompassing the three parts: resilience as a concept viewed by the country, its legislation background and institutional practices of crisis management/resilience response to current challenges. For the purpose of this Review, PROTECT used open sources of information collection as well as conducted expert focus group interviews in accordance with the elaborated Questionnaire (Annex 1).

Exclusively for the purpose of this Review, PROTECT designed a logic model of how to integrate some of the lessons learnt to the Ukrainian resilience system (Annex 2). Finally, based on the lessons learnt from other countries, the analysis contains general conclusions and PROTECT expert recommendations to the Government Office on European and Euro-Atlantic Integration about possible ways to integrate other countries' lessons learnt on resilience/crisis management systems into Ukrainian resilience systems.

1

NATO

The principle of resilience is anchored in **Article 3 of the Washington treaty**: “In order more effectively to achieve the objectives of this Treaty, the Parties, separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack.” Article 3 helps to give NATO the means to fulfil its core tasks, in particular, that of collective defence.

The **individual commitment** of each and every Ally to maintaining and strengthening its resilience reduces the vulnerability of NATO as a whole. Resilience is first and foremost a **national responsibility**. Each Ally needs to be sufficiently robust and adaptable to deal with and address the entire spectrum of crises envisaged by the Alliance.

Military efforts to defend Alliance territory and populations need to be complemented by robust civil preparedness to reduce potential vulnerabilities and the risk of attack in peacetime, crisis and conflict. Civil preparedness has three core functions: continuity of government, continuity of essential services to the population and civil support to military operations. These three critical functions have been translated into seven baseline requirements for national resilience against which Allies can measure their level of preparedness.

Military forces, especially those deployed during crises and conflict, heavily depend on the civilian and commercial sectors for transport, communications, energy and even basic supplies such as food and water, to fulfil their missions. Civil preparedness ensures that these sectors are ready to withstand external attacks or internal disruptions and remain able to provide support to a NATO military operation if needed.

Overall, NATO policy on resilience and civil preparedness is guided by the **Resilience Committee**, which reports directly to the North Atlantic Council, NATO’s principal political decision-making body.

At the **2016 NATO Summit in Warsaw**, Allied Leaders decided to boost NATO’s resilience to the full spectrum of threats and continue developing their countries’ individual and NATO’s collective capacity to resist any form of armed attack. They agreed **seven baseline requirements** for national resilience against which member states can measure their level of preparedness:

- Assured **continuity of government** and critical government services: for instance the ability to make decisions, communicate them and enforce them in a crisis;
- Resilient **energy supplies**: back-up plans and power grids, internally and across borders;
- Ability to deal effectively with **uncontrolled movement of people**, and to de-conflict these movements from NATO’s military deployments;
- Resilient **food and water resources**: ensuring these supplies are safe from disruption or sabotage;
- Ability to deal with **mass casualties and disruptive health crises**: ensuring that civilian health systems can cope and that sufficient medical supplies are stocked and secure;
- Resilient **civil communications systems**: ensuring that telecommunications and cyber networks function even under crisis conditions, with sufficient back-up capacity. This requirement was updated in November 2019 by NATO Defence Ministers, who stressed the need for reliable communications systems including 5G, robust options to restore these

systems, priority access to national authorities in times of crisis, and the thorough assessments of all risks to communications systems;

- Resilient **transport systems**: ensuring that NATO forces can move across Alliance territory rapidly and that civilian services can rely on transportation networks, even in a crisis.



These requirements reflect the **three core functions of continuity of government, essential services to the population and civil support to the military**, which must be maintained even under the most demanding circumstances. They are all connected, which means if one area is impacted, another may suffer as a result. Together with a package of resilience guidelines, evaluation criteria, assessments and a tailored toolbox, the objective of the baseline requirements is to support Allies in enhancing their resilience and to provide benchmarks against which to assess their state of civil preparedness.

In 2019, NATO leaders recognised the need to increase the **resilience of societies, as well as of the Allies' critical infrastructure and energy security**. They also committed to ensuring the security of communications, including 5G, recognising the need to rely on secure and resilient systems.

In 2021, Allied Heads of State and Government agreed a **Strengthened Resilience Commitment** to further enhance national and collective resilience and civil preparedness. Allies agreed to step up efforts to **secure and diversify supply chains; to ensure the resilience of critical infrastructure and key industries, including by protecting them from harmful economic activities; and to deal with the impact of natural hazards that are being exacerbated by climate change, among other commitments**.

Allies have also agreed to **establish, assess, review and monitor collective resilience objectives to guide nationally developed resilience goals and implementation plans**. This helps to build a more integrated and better-coordinated approach towards strengthening resilience at NATO. Supported by a new planning and review cycle, the national resilience goals are intended to operationalise the collective resilience objectives, the purpose of which is to address the Alliance's vulnerabilities across the seven baseline requirements.

In the para 10 of the Madrid Summit Declaration issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Madrid 29 June 2022, the Allies underlined:

“Resilience is a national responsibility and a collective commitment. We are enhancing our resilience, including through **nationally-developed goals and implementation plans**, guided by objectives developed by Allies together. We are also strengthening our energy security. We will ensure reliable energy supplies to our military forces. We will accelerate our adaptation in all domains, boosting our resilience to cyber and hybrid threats, and strengthening our interoperability. We will employ our political and military instruments in an integrated manner. We have endorsed a new chemical, biological, radiological and nuclear defence policy. We will significantly strengthen our cyber defences through enhanced civil-military cooperation. We will also expand partnership with industry. Allies have decided, **on a voluntary basis and using national assets, to build and exercise a virtual rapid response cyber capability to respond to significant malicious cyber activities.**”

Conclusion: According to decisions taken by Allies on the basis of consensus, resilience of Allied Nations is a national responsibility and a collective commitment. NATO Nations are enhancing their own resilience, including through nationally-developed goals and implementation plans, guided by objectives developed by Allies together.

European Union

Resilience

In the last decades, European society has been facing many different challenges. Society is being transformed by climate change, demographic imbalances, migration pressures and lately the Covid-19 pandemic.

Europe needs to further strengthen its resilience, to be able to be more prepared for future shocks and to emerge stronger by intensifying the transitions.

Resilience is a fundamental prerequisite for Europe as the largest integrated economic area in the world and has an important social dimension which requires the active cooperation of all stakeholders; citizens, the private sector, governments and NGOs included.

Resilience refers to the ability not only to withstand and cope with challenges but also to transform in a sustainable, fair, and democratic manner.²

Legislation

The [EU Strategic Agenda 2019-2024](#) pushes for a paradigm shift towards the green and digital transitions, leaving no one behind. It sets the basis for long-term strategic objectives in the context of the transition-led Commission agenda.

[Strategic foresight report](#) plays a key role in helping future-proof EU policymaking by ensuring that short-term initiatives are grounded in a longer term perspective. Strategic foresight can help build collective intelligence in a structured manner to better chart the way forward for the twin green and digital transitions and to recover from disruptions. Strategic foresight informs resilience-enhancing policies across four dimensions. It can help anticipate developments likely to have adverse impacts, to strengthen corresponding resilience through structural changes as well as taking into account the impact of current and future crises on relevant megatrends and emerging issues. Policies benefiting

² Manca, A.R., Benczur, P., and Giovannini, E., 2017, Building a scientific narrative towards a more resilient EU society

from strategic foresight can better mitigate the vulnerabilities and strengthen the capacities revealed by the crisis, opening new opportunities and making Europe more resilient.

The [dashboard](#) aims to capture social, economic, and health aspects related to COVID-19, using a first selection of easily available and ready-made indicators from publicly available data sources: the Social Scoreboard, and additional variables from Eurostat, Eurobarometer, the World Economic Forum's Global Competitiveness Index, the World Bank, the JRC, the European Institute for Gender Equality, the European Quality of Life Survey (EQLS), and research studies. Their novelty is rather in their multidimensional selection and resilience focus than in the creation of new indicators from raw data.

Links for documents:

1. [EU Strategic Agenda 2019-2024](#)
2. [2020 Strategic Foresight Report](#)
3. [Political guidelines of the Commission 2019-2024](#)
4. [Prototype dashboard for monitoring the social and economic dimension of resilience](#)
5. [Prototype dashboards for monitoring the geopolitical, green, and digital dimensions of resilience](#)

Four Dimensions of Resilience

Strategic Foresight Report outlines a view to strengthening the EU's resilience in four interrelated dimensions: social and economic, geopolitical, green, and digital.



Social and economic resilience

The pandemic has deepened inequalities, increased demographic imbalances and poverty, accelerated automation, and had a disproportionate impact on service sector jobs. Strategic foresight can be used to identify the skills for the future that we need to invest in now, and for having a larger societal conversation about updating the social and fiscal contract.

Geopolitical resilience

The crisis has highlighted the EU's over-reliance on third countries for critical raw materials crucial in key technologies needed to achieve a carbon-neutral and digital society. Strategic foresight can help identify possible scenarios and define strategic options to boost the EU's open strategic autonomy.

Green resilience

A shift to a greener economy could create 24 million new jobs globally and its impact in the recovery from the COVID-19 crisis could be significantly larger than previously thought. Strategic foresight can help us explore the drivers of change, understand the future structural shift in the labour market

and guide a reskilling of people who have lost their jobs during the crisis or who are likely to in the future due to technological developments and automation.

Digital resilience

The crisis has accelerated hyper-connectivity and the integration of new technologies affecting the human condition and the way we live. Strategic foresight can help us anticipate how key emerging technologies could develop, their impact on all spheres of life, and ways to seize upcoming opportunities.

Figure 1 shows one cycle of how strategic foresight can inform resilience-enhancing policies across the social and economic, geopolitical, green, and digital dimensions, taking into account the impact of the crisis on relevant megatrends. Policies benefiting from strategic foresight can better mitigate the vulnerabilities and strengthen the capacities revealed by the crisis, opening new opportunities and making Europe more resilient. This is a continuous process, with constant re-evaluation and feedback loops.

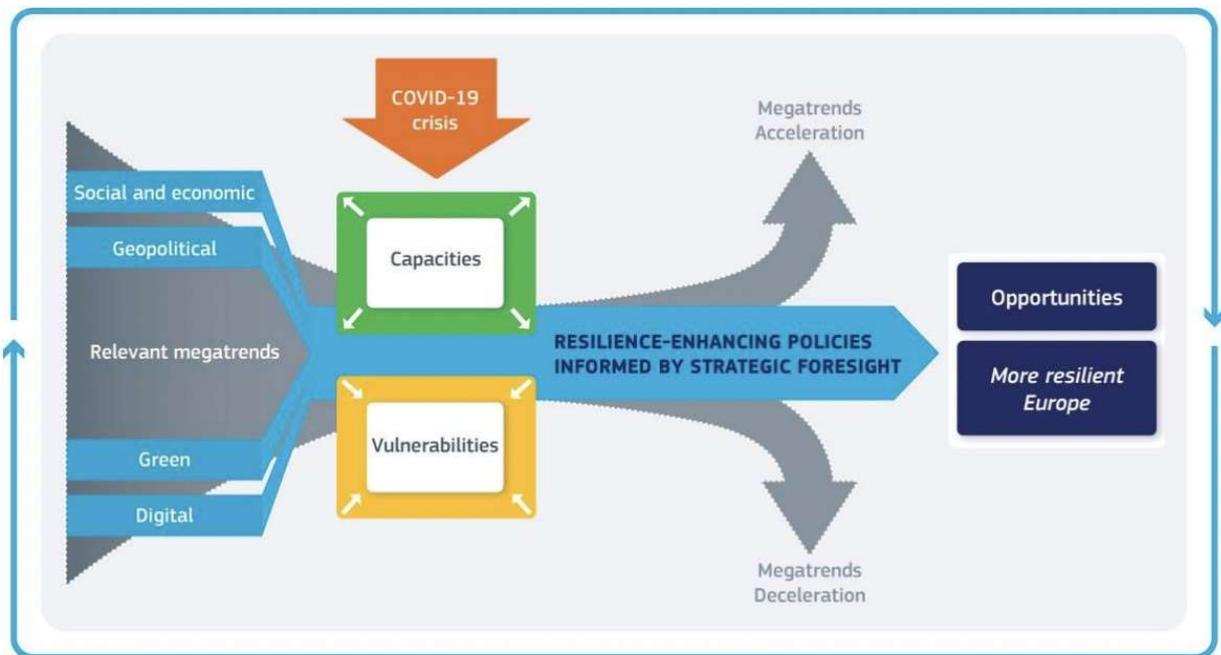


Figure 1: Link between strategic foresight and resilience³

Resilience dashboard

[This report presents the resilience dashboards](#) developed by the European Commission in a process of collective intelligence with Member States and other relevant stakeholders, as a follow up to the 2020 Strategic Foresight Report. The resilience dashboards are an innovative monitoring tool for the transition-led EU policy agenda. They provide a holistic assessment of the ability to progress amid challenges, across four dimensions: social and economic, green, digital, and geopolitical.

³ https://ec.europa.eu/info/sites/default/files/strategic_foresight_report_2020_1_0.pdf

The dashboards aim to capture vulnerabilities and capacities in the four dimensions: social and economic, green, digital and geopolitical.

Vulnerability: This is a country’s structural feature that points to elements of its systems (economic, social, and environmental) that can be disproportionately hit in the case of shocks and/or structural changes, or can hinder the transitions. A particular case is represented by vulnerable groups, defined as groups of people who would suffer a major loss from — and would have difficulties in coping with — the shock and/or undergoing the transitions. This could include, for example, people whose jobs are at a high risk of automation.

Capacity: This is a country’s structural feature that points to elements of its system (economic, social, and environmental) that are crucial for coping with shocks and/or structural changes, and managing transitions successfully. Examples include certain policies (e.g. active labour market policies), human and social capital (e.g. skills and digital competences), and the capacity to innovate through, for example, investment or innovative enterprises.

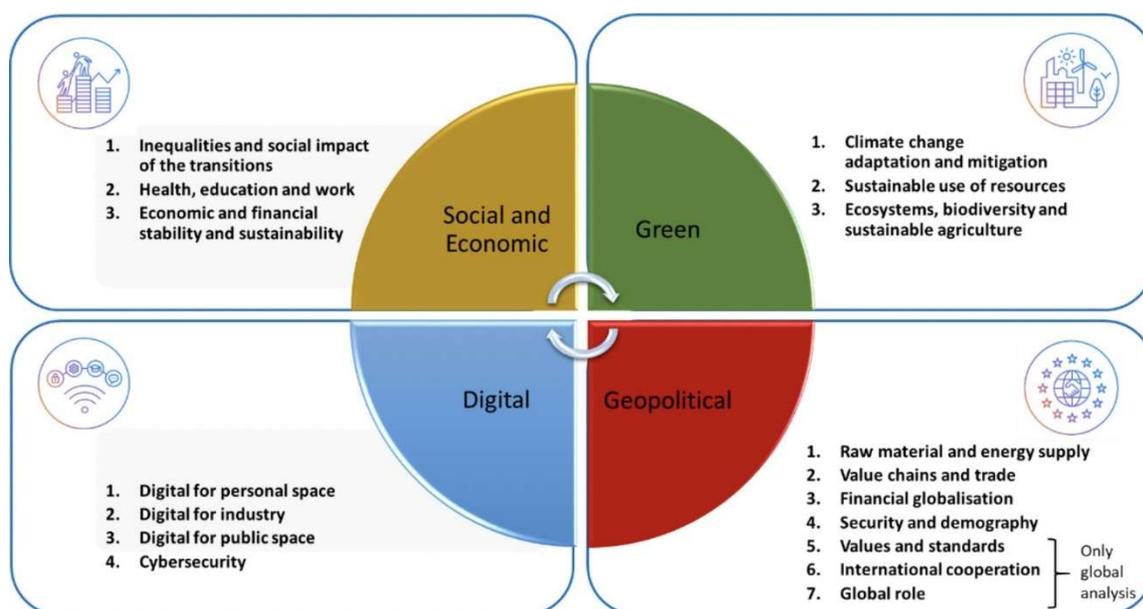


Figure 2: Areas covered in the four dimensions of the resilience dashboards⁴

Conclusions

In 2020, the central theme of the first annual Strategic Foresight Report is resilience. Resilience has become a new compass for EU policies with the COVID-19 crisis. It is the ability not only to withstand and to cope with challenges, but also to undergo transitions in a sustainable, fair, and democratic manner. The crisis has underscored the importance of future-proofing EU policies and of refocusing them around resilience.

The EU's resilience is presented in four interrelated dimensions: social and economic, geopolitical, green and digital. The resilience dashboards were presented aiming to capture social, economic, and health aspects related to COVID-19, using a first selection of easily available and ready-made indicators from publicly available data sources.

⁴ https://ec.europa.eu/info/sites/default/files/dashboard_report_20211129_en.pdf

Bulgaria

Resilience

The concept of resilience in a comprehensive security context remains primarily research and expert debate in Bulgaria. Compared to the concept of security, in which the main line of policy actions is between threats and vulnerabilities, resilience is seen as the opposite of vulnerability. The logic is that every effort to decrease any vulnerability automatically strengthens resilience. Due to the simplified understanding (organisational thinking), the "vulnerabilities" are seen chiefly as sectoral policy issues. However, such an interpretation is false; for example, diminishing vulnerability to climate change could not happen without industrial and agriculture reforms. This way of dominant thinking still limits the application of the resilience approach in Bulgaria. Ensuring resilience is seen primarily within individual comprehensive security' components rather than as an overarching and dominant concept.

Moreover, "resilience" is a broader concept than "security"; it is somehow a "next stage" of development. For example, information security, cyber defence, cyber security, and national cyber resilience are not only a ladder of development. They illustrate the necessary maturity of expert knowledge and political sense of strategic adaptability to cope effectively with future challenges. In Bulgaria, the former is in intensive building up, while the latter is still desirable.

However, using the concept of resilience in a national security context requires endless answering tough questions about the direction that implementation should take. What society we want to develop is still an open question in Bulgaria. The country needs to link resilience to other concepts to reflect national resilience's social, economic, security, and individual rights elements. The government should find various courses of action and develop relevant adaptation plans to build a national resilience system and culture gradually.

Legislation

Bulgaria has a set of laws on national security issues: *Law of the governance and functioning of the system for protection of the national security*, *Law for governance during crises*, *Law for protection in case of disasters*, *Law for the defense and the armed forces*, *Law for countering terrorism*, *Law for the State Agency "National Security"*, *Law for Defense Intelligence*, *Law for State Agency "Intelligence"*, *Law for Protection of Classified Information*, *Law for Preventing and Determining Conflict of Interests*, *Law for Access to Public Information*, *Law for the Consultative Council for National Security*.

Currently, the most comprehensive application of the concept of resilience in Bulgaria is the *National Recovery and Resilience Plan (2022)*. The ultimate objective of the Recovery and Resilience Plan is to facilitate economic and social recovery from the crisis caused by the COVID-19 pandemic and the ongoing economic, financial, and social consequences of the Russian war against Ukraine.

The Plan presents the views of the Government and the society on how recovery from the ongoing economic, social, and security difficulties should be addressed and overall national resilience achieved through an internally coherent and consistent combination of reforms and investments.

The European Commission adopted a positive assessment of Bulgaria's recovery and resilience plan on April 7, 2022 and paved the way to disburse €6.3 billion in grants under the Recovery and Resilience Facility (RRF)^[5].

In pursuit of this goal, the Government has established a set of measures and reforms that will not only restore the potential for economic growth, but will also develop it, which will allow, in the long run, to achieve an EU-average level of national resilience. At the same time, the Plan lays the foundations for a green and digital transformation of the economy, in the context of the ambitious goals of the Green Deal.

Institutions

Interagency interaction and coordination

The Constitutional spirit and arrangements envisage balanced roles and responsibilities for the national security, foreign, and defence policies between the divided democratic powers of the Parliament, President (Head of State and Supreme Commander of the Armed Forces) and the executive branch of government.

The institutions of the national resilience system are established in the respective laws based on the Constitution of the Republic of Bulgaria (1991). The hierarchy, functions and responsibilities are described in details in these high level normative acts.

Interaction with NATO

With the establishment in August 2013 CMDR CoE (Bulgaria, Greece and Poland), Sofia acquired a significant tool for improving its capabilities in crisis and disaster response operations through collaborative partnerships.

Conclusion

The analysis of open source information as well as focus expert group reports allows us to say that Bulgaria has a quite developed set of laws on national security issues. Bulgarian legislation in the field of national security and defence generally meets the requirements of the EU and NATO. At the same time there are no thematic laws that regulate the issue of Bulgaria's national resilience or national resilience system, while the concepts of building national resilience and creating a national resilience system are still at the stage of expert discussion.

The institutions of the national resilience system are established in the respective laws based on the Constitution of the Republic of Bulgaria. Bulgaria has elements of a national resilience system, as it is, but the system is not established in the country in full capacity. The system of interagency

⁵ [1] The RRF is the key instrument at the heart of NextGenerationEU. It will provide up to €800 billion (in current prices) to support investments and reforms across the EU. The Bulgarian plan forms part of an unprecedented coordinated EU response to the COVID-19 crisis, to address common European challenges by embracing the green and digital transitions, to strengthen economic and social resilience and the cohesion of the single market. Source https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2282

coordination in the field of security and defence was built in "pre-war" times, and doesn't fully take into account the factor of the all-encompassing Russian threat to Euro-Atlantic security and stability.

One gets the impression that Bulgaria relies more on NATO and EU mechanisms to ensure national resilience, stability and security than on its own strength and capabilities while despite the long catalogue of services the capacity of the CMDR CoE is not fully utilised yet.

Estonia

Resilience

Resilience concepts are developed for critical infrastructures such as the supply of basic services like water, food, energy, transport, housing, communications, etc.

Resilience concepts need also to take into account the necessity to anticipate, to plan and to implement in the crises time a substitution process aiming to deal with a lack of material, technical or human resources or capacities necessary to assume the continuity of basic functions and services until recovery from negative effects and until return to the nominal position.

The Estonian crisis management system is based on measures that can be taken in order to protect human life, property and the environment during civil emergencies.⁶

Estonia has signed regional and multilateral provisions of the Council of Europe, the EU, the NATO and the OSCE for assistance in crisis situations. Estonia is also an active initiator in the field of maritime cooperation and of strategic and operational dialogue among the Baltic Sea countries.

Estonia has built its current level of cybersecurity maturity over the past 12 years through the continuous and systematic development and implementation of three iterations of national cybersecurity strategy. The country prepared a new version of this strategy closely tied to its digital development agenda and assessing the lessons from previous periods.

Legislation

*The National Security Concept of the Republic of Estonia*⁷ is a key document that establishes the objectives, principles and directions of security policy. The National Security Concept highlights crisis management as one of the essentially important tasks.

The main task of Crisis Management⁸ is to ensure the readiness for implementation of the Cybersecurity Act and the Emergency Act: planning and management on a national as well as

⁶

<https://isij.eu/article/estonia-capabilities-organisations-policies-and-legislation-crisis-management-and-disaster>

⁷

https://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_security_concept_2017_0.pdf

⁸ <https://www.ria.ee/en/cyber-security/crisis-management.html>

international level. On August 16, 2022, an updated version of the Cybersecurity Act⁹ was published (English translation is currently unavailable).

Another important conceptual document is the *Strategy of the Estonian Rescue Board 2015-2025*¹⁰ which plans the Board's activities in a ten year timeframe.

The main regulatory framework for civil protection and emergencies is defined by the *Emergency Act*¹¹ and the *Rescue Act*¹².

Quote from the Concept of National Security – Chapter 3.8 "Resistance and Cohesion of Society"¹³:

"The more united a society and the more common values it shares, the less it can be influenced and the less susceptible it is to security threats. The more residents trust the state, the more resilient it is. Trust increases when the state takes responsibility for the well-being of its people and prepares for coping with security threats and risks. Strategic communication is important in determining society's values and facilitating people's readiness to contribute to it.

The cohesion of society is improved by tolerant, caring and inclusive understandings, the strong integration of different segments of society, and uniform regional development. The resilience of society develops through the joint influence of credible civil protection, people's psychological strength, and a safe social and physical living environment. All these areas need constant attention and development; for some, global processes must be understood, while society has to adapt and adjust to them; some fields have a broader influence in the region.

The national security is influenced by economic, social and environmental factors across Estonia. Life must be habitable and safe everywhere in Estonia. Unfavourable demographic processes and the excessive accumulation of major socio-economic, security and safety risks in certain regions must be avoided or prevented. To guarantee uniform regional development and even population distribution, the government develops the infrastructure; supports the improvement of the performance of local governments; promotes civil society and voluntary action; and ensures public safety, the availability and quality of education, healthcare and other public services, as well as the comprehensive management of regional policy. Regional characteristics will be considered in providing state services. State agencies and local governments must cooperate more effectively to cope with society related security risks.

Cohesive society is less vulnerable and less open to the influences from outside. The better integration of society will reinforce unity and cohesion. The purpose of integration in Estonia is to shape a culturally versatile society that has a strong identity and shares common values. The state will continue activities that facilitate the adjustment and integration of different groups in society to develop and improve the people's willingness and opportunities to participate actively in societal life. Integration is more effective through uniform regional development, equal access to high-quality education, promotion of instruction in the national language, making a variety types of support

⁹ <https://www.riigiteataja.ee/akt/106082022018>

¹⁰ https://www.rescue.ee/files/2018-10/1540892641_srateegia-eng-web.pdf

¹¹ <https://www.riigiteataja.ee/en/eli/ee/513062017001/consolide/current>

¹² <https://www.riigiteataja.ee/en/eli/528062022006/consolide>

¹³

https://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_security_concept_2017_0.pdf, page 19

service available, and adaptation of new migrants to the society. The activity and cooperation of civil society, local governments and state agencies helps to shape a favourable environment for adjustment and integration. Excessively divergent views and unbalanced criticism of diversity damages the cohesion and resilience of society. The state must focus more on the equal treatment of the most vulnerable segments in society, protecting their fundamental rights and creating a liveable environment for them.

The cohesion and integration, as well as the resilience, of society can be reinforced if the population is better and more reliably informed. Strategic communication involves planning the state's political, economic and defence-related statements and activities, preparing a comprehensive informative whole on the basis of these, and transmitting it to the population. It is based on the nation's values expressed in a democratic, versatile and deep dialogue, which the government will follow in serving society. The main objective of strategic communication — the resilience and better cohesion of society — cannot be achieved by political declarations alone; it comes about due to the combined influence of many factors. As a result, the living environment will grow more stable and secure, and the vulnerability of society (due also to security threats) will decrease.

Psychological defence is about informing society and raising awareness about information related activities aimed at harming Estonia's constitutional order, society's values and virtues. Psychological defence is needed to neutralise attacks by terrorist organisations as well as assaults proceeding from the military doctrine of certain states with the help of efforts to influence the society under attack with cognitive methods. Appropriate measures must be drawn up for this. The purpose of psychological defence is to prevent crises in Estonia, facilitate security awareness in society and neutralise information attacks that provoke violence in the population by manipulation and the provision of false information, or that promote crisis management with resources that are not compatible with constitutional order. The best tool of psychological defence is to inform the public of attacks, manipulation and false information and guarantee access to multifaceted information for all segments of society. Psychological defence is developed in cooperation with civil society.

Strategic communication and psychological defence complement one another. While the notification methods of psychological defence are mostly reactive, strategic communication must be able to reach society as well as foreign target groups, which play an important part in conflict management in the context of the greater information noise generated during a conflict. To achieve this, networks of people and the media must provide their support".

Institutions

In Estonia the highest authority responsible for emergency and disaster management is the Ministry of Interior. It is responsible for policy formulation and its execution in the area of civil security. At regional level county governors are directly responsible to the Minister of the Interior for crisis management matters. The county governor is the highest crisis management authority at regional level. At the local level the main body responsible for civil protection is the local government council which has established the local crisis management committee chaired by the mayor.

The Estonian Rescue Board is directly subordinate to the Ministry of Interior and has a key role in representing Estonia in various international forums such as the UN, EU and NATO and other relevant civil security organisations. Another national government institution under the authority of the Ministry of Interior is the Emergency Response Centre responsible for processing emergency calls to the emergency 112 number and sending out rescue teams to the place of the emergency.

As in the other Baltic Region States the organisational structure is centralised, i.e. coordinated and mostly organised by the central national civil protection authority, as is the case with Estonia, Latvia, Lithuania. Additionally, the use of private rescue services is low in the Baltic Countries.

The Defence Forces could be deployed in response to a crisis or disaster, but in cases where all the other crisis management capabilities of the state have been exhausted or where the required resources or capabilities are only available to the Defence Forces.

In addition, Crisis Management organises the national resolution of extensive cyber incidents. The Information System Authority (RIA) ensures readiness for resolving crises caused by cyber incidents by:

- developing and implementing preparedness procedures for internal as well as trans-institutional and international use
- organising national and international crisis and cyber exercises in cooperation with partner institutions and companies
- coordinating the prevention and resolution of cyber crises by advising companies and state authorities who provide vital and essential services
- conducting civilian-military cyber cooperation together with the Defence Forces and the Defence League.

Conclusions

The resilience capability of Estonia to prevent and avert security threats depends on the readiness to maintain critical services. In promoting and enhancing resilience concepts, the state cooperates and involves other members of civil society, thus improving social cohesion and social risks are prevented. The prevention of social risks is addressed in the national economic and social policy.

In order to ensure the resilience of critical services, Estonia develops operational capability to recover interrupted services, provides sufficient reserves and action plans. Continuous evaluation and monitoring of risks that may disrupt or cause malfunction in critical services is conducted.

Moreover, to safeguard the state's resilience, a plan for organising the functioning of national command and control and guaranteeing continuity of government in the event of risk situations and crises shall be drafted under the co-ordination of the Ministry of Defence. The Rescue Board also develops emergency plans and maintains the resilience of the country.

The concept of Resilience has been introduced into the legislative space of Estonia in the National Security Concept in 2017.

The National Security Concept defines the objective, principles and course of action of Estonian security policy. The document has been prepared by the Government of the Republic and approved by the Parliament (Riigikogu). As a framework document it provides guidance for drafting national development and action plans. The Concept is amended or reviewed pursuant to changes in the security environment and developments of the Estonian national security system, but each composition of the Riigikogu shall update the Concept at least every four years. At least twice

during the four-year cycle the Prime Minister shall inform the Riigikogu about achieving the goals set in the concept. Estonia addresses its security as a part of a wider international security. In maintaining its security, Estonia seeks and supports ways and means that have a positive impact on Estonia as well as on other states.

"Estonia's approach is based on the conviction that security is generated to protect human rights, fundamental freedoms and basic human values. These values determine our way of life and Estonia represents them in general. When we honour democratic principles, our society can last and develop in a constant and sustainable manner. In this way, a viable civil society and the people's will to defend Estonia will grow stronger and Estonia's position and reputation in the world will improve".¹⁴

Finland

Resilience

In recent years, Finnish government has begun to increase societal resilience and preparedness to manage interconnected security risks and complex crises. These range from the climate disaster to migration, disinformation and transnational terrorism to food insecurity, natural catastrophes, pandemics and conventional inter-state war and beyond.

The [National Security Overview 2021](#) outlines the following security risks:

Intelligence and influencing operations targeting Finland. Finland and its population are continually subject to a broad range of unlawful intelligence operations. Finland remains a target of intelligence interest to Russia and China in particular.

Cyber threats to national security can arise in the form of cyber espionage or influence by foreign powers. The side effects of cybercrime may also pose a threat to national security as society becomes increasingly dependent on the smooth operation of information systems.

Terrorism. The main threat of terrorism in Finland is posed by individuals and small groups supporting far-right or radical Islamist ideologies. The number of CT targets has remained unchanged at about 390.

Threats to critical infrastructure. Critical infrastructure is a long-term target of foreign intelligence operations in Finland. Authoritarian states can also access Finland's critical infrastructure through legitimate activities, such as business acquisitions and joint ventures.

Dual-use products and weapons of mass destruction. Parties seeking to procure weapons of mass destruction and components of such weaponry have directed efforts through Finland and Finnish operators.

Finland has applied for membership in the North Atlantic Treaty Organization (NATO) in 2022. NATO membership would strengthen Finland's security as well as the security and stability of the Baltic Sea region and Northern Europe. Finland has taken an active part in civil preparedness and resilience cooperation since Finland became a partner for peace. The civil preparedness issues for which the Ministry of the Interior is responsible are part of NATO's new resilience policy defined in the NATO 2030 agenda. NATO's Resilience Committee, which started its work in May 2022, guides this work in NATO. This Committee will generate a significant workload for the Ministry of the Interior's branch of government, among others.

¹⁴ https://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_security_concept_2017_0.pdf

Finland will be able to take part in the exchange of military and civilian intelligence. National security and intelligence are an important policy area in NATO.

The Security Strategy for Society lays out the general principles governing preparedness in Finnish society. The concept for Comprehensive Security is the Finnish model of cross-governmental preparedness, where authorities, businesses, NGOs, and citizens are jointly responsible for safeguarding society's vital functions. The aim is that during whichever type of crisis, the entirety of Finnish Society is able to rapidly mobilize resources where needed, recover quickly, and adapt its functions based on the lessons learned.

The vital function of society defined in the Security Strategy for Society is security of supply. Security of supply means the safeguarding of the critical production, services and infrastructure necessary for the livelihood of the population, the national economy and the national defence in cases of serious incidents and emergencies.

Legislation

Baselines of the Finnish Concept of Comprehensive Security are described in the [Security Strategy for Society \(2017\)](#). The Security Strategy for Society 2017 is a government resolution that harmonises the set of national principles regarding preparedness and guides the preparedness actions taken by the administrative branches.

In the core of the Strategy are Seven Functions Vital for Society presented in the figure 1:



Figure 1: The functions vital to society¹⁵

In Finland, Rescue Services operate under the Rescue Act (379/2011) and other similar acts. The Rescue Act lays down the responsibilities of various parties in performing rescue service duties and aims to prevent accidents and limit the consequences of accidents.

¹⁵ https://turvallisuuskomitea.fi/wp-content/uploads/2018/04/YTS_2017_english.pdf

Preparedness is based on the preparedness obligation laid down in the Emergency Powers Act (1552/2011), the Rescue Act and other legislation. According to the Rescue Act, emergency preparedness planning and cooperation is the duty of the rescue services authorities.

The Government Decision on the Objectives of Security of Supply (1048/2018) defines the starting points, principles and national objectives of the national security of supply measures to ensure the implementation of security of supply in a constantly changing operating and security environment.

Links for documents:

1. [SECURITY STRATEGY FOR SOCIETY, Government Resolution / 2.11.2017](#)
2. [Government Decision on the Objectives of Security of Supply \(1048/2018\)](#)
3. [Emergency Powers Act \(1552/2011\)](#)
4. [Rescue Act \(379/2011\)](#)
5. [The National Security Overview 2021](#)
6. [Presentation of the Finnish Concept for Comprehensive Security](#)

Institutions

The fact that the comprehensive security model applied in Finland covers all levels and actors of society is its strength. Together with the central government, the authorities, business operators, regions and municipalities, such actors as universities, research institutions, organisations, other bodies and individuals form a network of comprehensive security in which the sharing of information, setting of joint objectives and commitments to cooperation can take place in a flexible manner.

Vital functions of society cover the statutory tasks of a large number of actors in a cross-sectoral manner and they also include areas where the responsibility is shared by several parties.

Leadership

Prerequisites of the state leadership Ministry in charge: Prime Minister's Office

2. **Maintaining the situation picture of the state leadership** Ministry in charge: Prime Minister's Office

3. **Functioning of communications** Ministries in charge: Prime Minister's Office and all other ministries

International and EU activities

4. **Finland's role in the European Union; ensuring that EU matters can be properly drafted and considered at national level and securing solidarity and mutual assistance** Ministries in charge: Prime Minister's Office and all other ministries

5. **Developing contacts and cooperation with foreign countries and key international actors** Ministries in charge: Ministry for Foreign Affairs and all other ministries in their own areas of responsibility
6. **International crisis management, humanitarian assistance and international rescue operations** Ministries in charge: Ministry for Foreign Affairs, Ministry of Defence, Ministry of the Interior, Prime Minister's Office, Ministry of Social Affairs and Health, Ministry of Justice
7. **Providing Finnish citizens and foreigners permanently residing in Finland with protection and assistance outside Finland** Ministry in charge: Ministry for Foreign Affairs
8. **Ensuring a smooth flow of goods and services between Finland and other countries** Ministries in charge: Ministry for Foreign Affairs, Ministry of Economic Affairs and Employment, Ministry of Agriculture and Forestry, Ministry of Transport and Communications, Ministry of Finance

Defence capability

9. **Finland's military defence** Ministry in charge: Ministry of Defence

Internal security

10. **Ensuring legal protection** Ministry in charge: Ministry of Justice
11. **Holding elections and safeguarding the prerequisites of democracy** Ministry in charge: Ministry of Justice
12. **Maintaining public order and security** Ministry in charge: Ministry of the Interior
13. **Ensuring border security** Ministry in charge: Ministry of the Interior
14. **Ensuring the safety of supply chains and safety of goods** Ministry in charge: Ministry of Finance
15. **Civil defence** Ministry in charge: Ministry of the Interior
16. **Ensuring the maritime search and rescue capability** Ministry in charge: Ministry of the Interior
17. **Emergency response centres** Ministries in charge: Ministry of the Interior, Ministry of Social Affairs and Health
18. **Maintaining rescue services** Ministry in charge: Ministry of the Interior
19. **Immigration control** Ministries in charge: Ministry of the Interior, Ministry for Foreign Affairs, Ministry of Economic Affairs and Employment
20. **Management of large-scale immigration** Ministries in charge: Ministry of the Interior and Ministry of Economic Affairs and Employment
21. **Environmental emergency response** Ministries in charge: Ministry of the Environment, Ministry of Transport and Communications, Ministry of Economic Affairs and Employment, Ministry of the Interior, Ministry of Defence
22. **Preparedness for biological threats** Ministries in charge: Ministry of Social Affairs and Health, Ministry of Agriculture and Forestry, Ministry of Defence, Ministry for Foreign Affairs, Ministry of the Interior, Ministry of the Environment
23. **Preventing radiation hazards and preparing for them** Ministries in charge: Ministry of the Interior, Ministry of Social Affairs and Health, Ministry of Agriculture and Forestry, Ministry of the Environment, Ministry of Defence, Ministry of Economic Affairs and Employment
24. **Preparation for chemical threats** Ministries in charge: Ministry of Social Affairs and Health, Ministry of the Interior, Ministry of Economic Affairs and Employment, Ministry of Agriculture and Forestry, Ministry of the Environment, Ministry of Defence

Economy, infrastructure and security of supply

25. **Acquiring economic resources and focusing them and safeguarding human resources** Ministry in charge: Ministry of Finance
26. **Ensuring the functioning of the financial system** Ministry in charge: Ministry of Finance
27. **Safeguarding public administration ICT infrastructure and digital services** Ministries in charge: Ministry of Finance, Prime Minister's Office
28. **Ensuring availability of and access to electronic communications services** Ministry in charge: Ministry of Transport and Communications
29. **Safeguarding the continuation of insurance business** Ministry in charge: Ministry of Social Affairs and Health
30. **Securing the fuel supply** Ministries in charge: Ministry of Economic Affairs and Employment, Ministry of Transport and Communications, Ministry of Agriculture and Forestry
31. **Securing power supply** Ministry in charge: Ministry of Economic Affairs and Employment
32. **Ensuring weather, maritime and circumstance services** Ministry in charge: Ministry of Transport and Communications
33. **Ensuring the availability and usability of transport services** Ministry in charge: Ministry of Transport and Communications
34. **Ensuring the security and operational reliability of transport and communications network** Ministry in charge: Ministry of Transport and Communications
35. **Ensuring the continuity of the transports essential for Finland's security of supply and foreign trade** Ministries in charge: Ministry of Transport and Communications, Ministry of Defence, Ministry of Economic Affairs and Employment
36. **Ensuring the functioning of the social welfare and health care information systems and the availability of critical supplies** Ministries in charge: Ministry of Social Affairs and Health, Ministry of Economic Affairs and Employment
37. **Detection and monitoring of changes taking place in the environment, adapting to the changes and combating the threats arising from them** Ministries in charge: Ministry of the Environment, Ministry of Agriculture and Forestry
38. **Ensuring waste management** Ministry in charge: Ministry of the Environment
39. **Securing resources for construction** Ministry in charge: Ministry of the Environment
40. **Ensuring proper housing** Ministry in charge: Ministry of the Environment
41. **Safeguarding the water supply** Ministries in charge: Ministry of Agriculture and Forestry, Ministry of Social Affairs and Health, Ministry of the Environment
42. **Flood risk management and supervision of dam safety** Ministry in charge: Ministry of Agriculture and Forestry
43. **Securing sufficient labour workforce** Ministry in charge: Ministry of Economic Affairs and Employment
44. **Maintaining the education, training and research system** Ministry in charge: Ministry of Education and Culture
45. **Safeguarding vital industries and services** Ministry in charge: Ministry of Economic Affairs and Employment

46. **Safeguarding food supply** Ministries in charge: Ministry of Agriculture and Forestry, Ministry of Economic Affairs and Employment, Ministry of Transport and Communications, Ministry of Social Affairs and Health, Ministry for Foreign Affairs
47. **Ensuring the supply of daily consumer goods** Ministries in charge: Ministry of Economic Affairs and Employment, Ministry of Agriculture and Forestry

Functional capacity of the population and services

48. **Ensuring the last-resort livelihood of the population** Ministries in charge: Ministry of Social Affairs and Health, Ministry of Finance
49. **Ensuring access to social welfare and health care services** Ministry in charge: Ministry of Social Affairs and Health
50. **Maintaining expertise and skills** Ministry in charge: Ministry of Education and Culture

Psychological resilience

51. **Maintaining cultural services and protecting cultural heritage** Ministry in charge: Ministry of Education and Culture
52. **Ensuring the basis for religious activities** Ministry in charge: Ministry of Education and Culture
53. **Ensuring the continuation of youth work and activities as well as civic sports activities** Ministry in charge: Ministry of Education and Culture
54. **Communications** Ministries in charge: all ministries
55. **Combating social exclusion and inequality** Ministries in charge: Ministry of Social Affairs and Health, Ministry of Education and Culture, Ministry of Economic Affairs and Employment
56. **Promoting voluntary activities** Responsible actors: all administrative branches and organisations
57. **Recovery** Responsible actors: all administrative branches and organisations

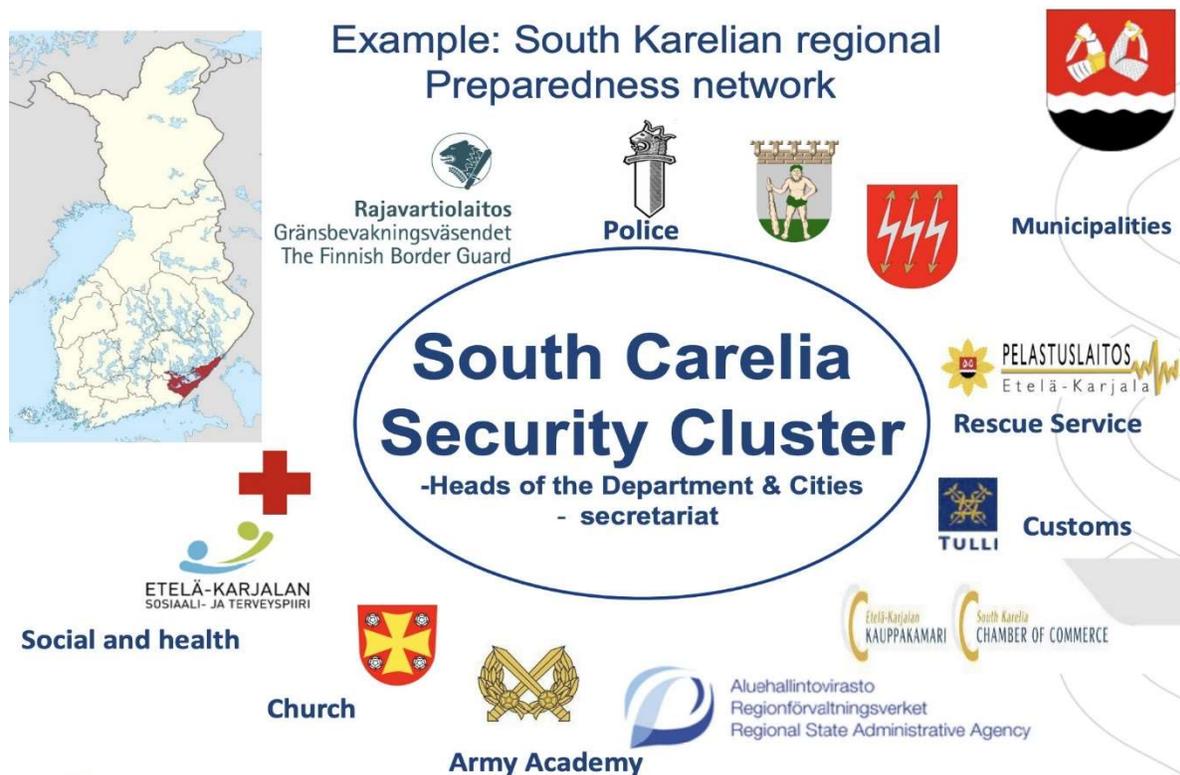
Preparedness, obligation of public administration, independent preparedness of business operators, other bodies and households is an important part of Finland's resilience. Public administration actors and other bodies draft their preparedness plans within the framework of comprehensive security.

PREPAREDNESS PROCESS



Figure 3: General preparedness process¹⁶

In the model (figure 4), all actors taking part in coordinated security work or security activities closely supporting it are security actors. Individual citizens also play an important role in independent preparedness and in enhancing the resilience of Finnish society.



¹⁶ https://turvallisuuskomitea.fi/wp-content/uploads/2018/04/YTS_2017_english.pdf

Figure 4: The South Karelian regional Preparedness network¹⁷

The Security Committee assists the Government in comprehensive security preparedness and in its coordination. The Security Committee monitors the implementation of the Security Strategy for Society, developments in the security environment and the level of preparedness in individual administrative branches (figure 5).

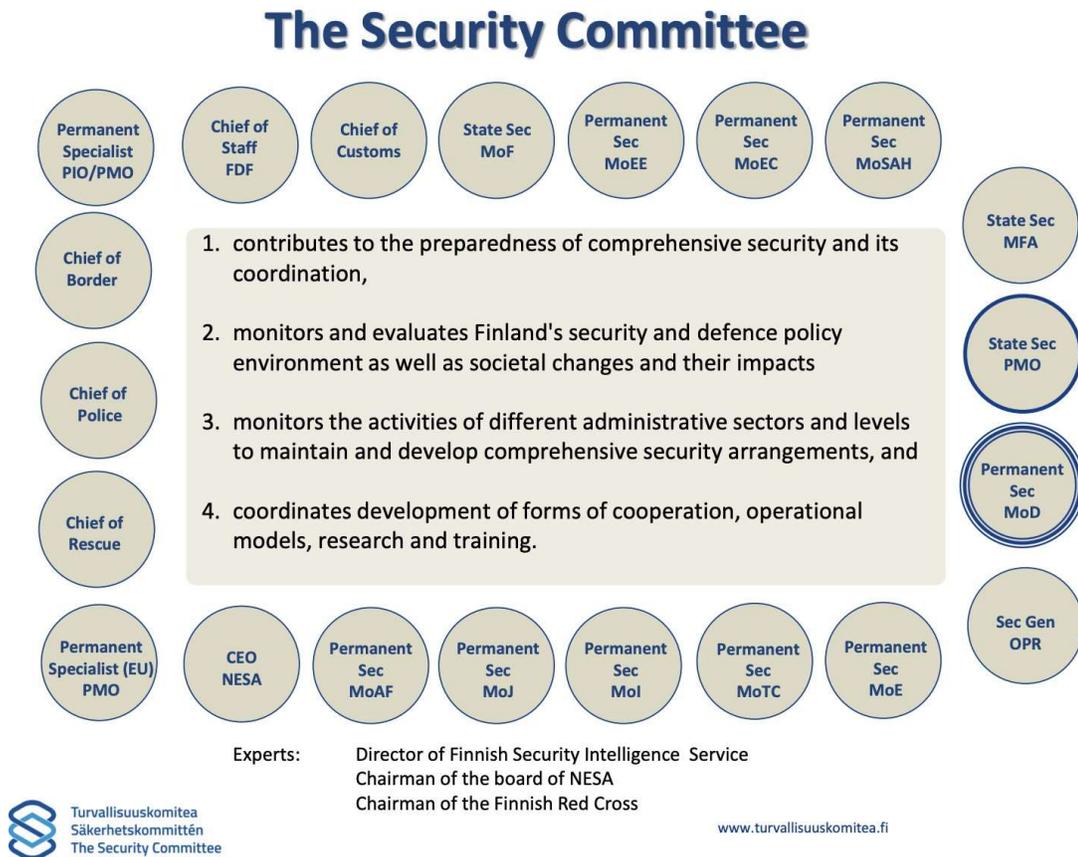


Figure 5: The Security Committee¹⁸

The security environment and changes in it are discussed in the security reports produced by the Government and in the assessments produced by individual actors and administrative branches. For example, change trends in internal security are described in the Internal Security Strategy.

¹⁷

https://www.defmin.fi/files/3827/Valtonen_2017_06_14_FI_Concept_for_Comprehensive_Security_Valtonen.pdf

¹⁸

https://www.defmin.fi/files/3827/Valtonen_2017_06_14_FI_Concept_for_Comprehensive_Security_Valtonen.pdf

Preparedness cooperation bodies must make effective use of the risk analyses and analyses of the operating environment relevant to their areas of responsibility. The participants must supplement the analyses with their own assessments.

The national risk assessment of 2015 was based on the European Union legislation on the civil protection mechanism. It was drawn up in a cross-administrative project managed by the **Ministry of the Interior and steered by the Security Committee**.

SSfs 2010	NATIONAL RISK ASSESSMENT 2015	NATIONAL RISK ASSESSMENT 2018
<p>Threat scenarios:</p> <ul style="list-style-type: none"> • Serious disruptions to power supply • Serious disruptions to telecommunications and information systems • Serious disruptions to transport logistics • Serious disruptions to public utilities • Serious disruptions to food supply • Serious disruptions to financial and payment systems • Disruptions to the availability of public funding • Disruptions to the health and welfare of the population • Major accidents, extreme natural phenomena and environmental threats • Terrorism and other crime that endanger social order • Serious disturbances in border security • Political, economic and military pressure • Use of military force 	<p>Wide-ranging events affecting society:</p> <ul style="list-style-type: none"> • Serious disruptions to energy supply • Risks in the cyber domain • Serious human infectious diseases, worldwide and in our vicinity • A security policy related crisis which directly or indirectly affects Finland • A serious nuclear accident in Finland or in our vicinity • Solar storm <p>Serious regional events:</p> <ul style="list-style-type: none"> • Extensive rapid flooding in or around urban areas • A serious chemical accident or explosion at a plant handling dangerous substances • A major maritime accident • A major aviation accident • A major rail transport accident • A major road traffic accident • Several simultaneously occurring major forest fires • A major building fire at infrastructure critical to society • An extensive or extended disruption in water supply • A large-scale winter storm followed by a long cold spell • A severe thunderstorm • A terrorist act or terrorism targeting Finland • A serious act of violence targeted at crowds • Violent, large-scale civil disturbances • A mass influx of migrants 	<ul style="list-style-type: none"> • Updated every three years • Will be expanded as required by the Security Strategy for Society • Provides the basis for preparedness planning at all levels of activity

Figure 6: Threat and risk scenarios and the national risk assessment to be updated every three years¹⁹

¹⁹ https://turvallisuuskomitea.fi/wp-content/uploads/2018/04/YTS_2017_english.pdf

Modelled on how the state leadership acts in such situations (figure 7), the general principles applied to the management of incidents are also observed at regional and local level. In regions and municipalities, the priority is on what is required at the local level. The lines of authority and the principles governing the compilation and sharing of the situation picture will be of central importance in the management of municipalities and the regions to be established as part of the social welfare, health care and regional government reform.

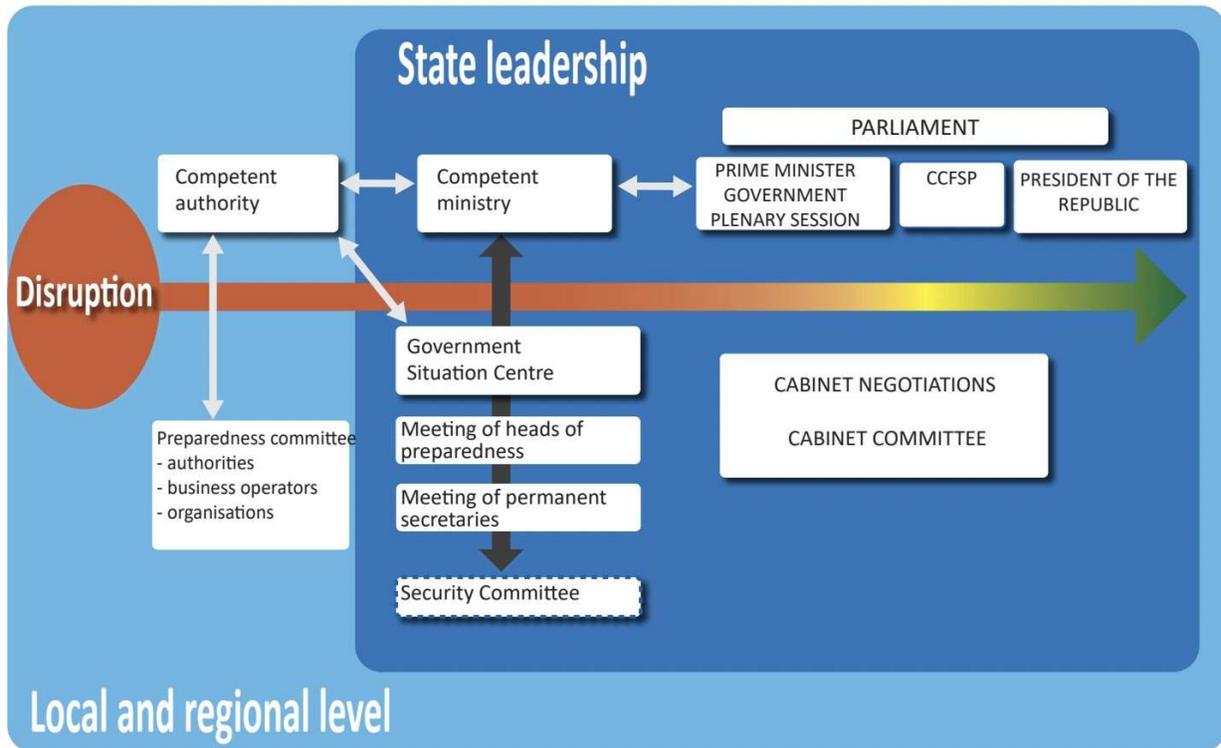


Figure 7: A general functional model for leadership and managing incidents²⁰

Conclusions

The Security Strategy for Society is a government resolution that harmonises the set of national principles regarding preparedness and guides the preparedness actions taken by the administrative branches. The Security Strategy for Society was drawn up through broad-based cooperation, taking into account the viewpoints of all actors. Since comprehensive security is built in cooperation it involves the authorities, the business life, NGOs and communities, and citizens. Each administrative branch is responsible for implementing the Strategy within its competence. The Security Committee monitors the Strategy's implementation and coordinates cooperation measures together with the ministries' Heads of Preparedness. The Strategy clearly outlines vital functions of: the Leadership; International and EU activities; Defence capability; Internal security; Economy, infrastructure and security of supply; Functional capacity of the population and services; Psychological resilience as well as Risk assessment as a basis for preparedness. The threat and risk scenarios and the national risk assessment to be updated every three years. The Department for Rescue Services at the Ministry of the Interior is in charge of the organisation of rescue services at national level, guides and directs rescue services, and coordinates the activities of various ministries and sectors

²⁰ https://turvallisuuskomitea.fi/wp-content/uploads/2018/04/YTS_2017_english.pdf

in the field of rescue services and their development. The Emergency Response Centre Administration is an agency under the Ministry of the Interior. The Ministry of Economic Affairs and Employment is responsible for the development and coordination of the security of supply measures.

Lithuania

Resilience

The term Resilience is not used in Lithuanian policy or legislative documents. No information has been found referring to the resilience concept addressing crises, disasters, crisis management or other related topics.

The Lithuanian organisational structure is centralised, i.e. coordinated and mostly organised by the central national civil protection authority.

The National Security Strategy establishes the basic goals and means of the national security policy. The aim of the Lithuanian National Security Strategy is to provide a vision of the state's development, its national interests and the necessary actions for their implementation.

The Civil Security System and the Civil Protection System of Lithuania is comprised by the Government, the state and municipal institutions, economic entities, public organisations, civil protection forces such as fire and rescue, police, state border guard, medical services, public security service, state food and agriculture service, other emergency services, forces of economic entities, volunteers, the emergency commissions and emergency operation centres.

Legislation

1. Constitution of Republic of Lithuania²¹
2. The Law on Basics of National Security²²
3. National Security Strategy of the Republic of Lithuania²³
4. Law on the Protection of Objects of Importance to Ensuring National Security²⁴
5. The Civil Protection Law of Lithuania²⁵
6. Lithuania: Capabilities, Organisations, Policies, and Legislation in crisis management and disaster response²⁶

²¹ <https://e-seimas.lrs.lt/portal/legalActPrint/lt?ifwid=rivwzvpng>

²² <https://e-seimas.lrs.lt/portal/legalActPrint/lt?ifwid=9tq147ume&documentId=TAIS.39790&category=TAD>

²³ <https://www.newstrategycenter.ro/wp-content/uploads/2019/07/2017-nacsaugstrategijaen.pdf>

²⁴ <https://investmentpolicy.unctad.org/investment-laws/laws/>

²⁵ <http://extwprlegs1.fao.org/docs/pdf/lit195280.pdf>

²⁶ <https://isij.eu/article/lithuania-capabilities-organisations-policies-and-legislation-crisis-management-and-disaster>

The National Security Strategy establishes the basic goals and means of the national security policy. The aim of the Lithuanian National Security Strategy is to provide a vision of the state's development, its national interests and the necessary actions for their implementation.

Further, the Strategy defines the basic goals of specialised strategies and doctrines in relevant areas of state policy. These strategies have to be based on the provisions of the National Security Strategy and must be revised every time the National Security Strategy of Lithuania is updated.

Conflict prevention is one of the Strategy's main priorities, more particularly participating in international crisis management and establishing policies and legislation to address new security challenges, dangers and threats.

Additionally, the Strategy foresees cooperation with NATO Member states to further strengthen regional security, in order to consolidate the national security system of the Republic of Lithuania and reinforce national and international crisis management capabilities.

The Strategy also highlights the readiness of Lithuanian forces for participation in international peace operations, crisis management and prevention. The Strategy also underlines the importance for the establishment of a crisis management system in Lithuania in order to ensure effective detection and prevention of threats, as well as the national security in the area of crisis management. The system is being established for functioning in the pre-crisis situations, ensuring comprehensive monitoring of dangerous situations and threats, crisis detection, preparation and implementation of preventive measures.

The main means and measures for improving crisis management and response capabilities include: enhancing the preventive role of the crisis management system for detecting and eliminating emergency situations and threats; establishing civil safety and rescue institutions for managing crisis situations and to ensure immediate emergency aid in the case of fire, industrial disaster or another incident

The Civil Protection Law of Lithuania establishes legal and organisational principles for the organisation and operation of the civil and rescue system, along with the duties and rights of state and municipal institutions, economic entities, public organisations and residents.

The goals of the civil protection and rescue system include guaranteeing the optimum use of state resources in order to ensure public security, maintain the operability of the national economy, localise the emergency areas and mitigate the effects thereof; preparing the public for practical actions in the event of an emergency and strengthen the confidence in the activity of civil protection and rescue system.

The main tasks of Civil Protection and Rescue System in Lithuania, considering the causes, the type and threat of the emergencies, encompass: warning the population of the emergency, the possible effects and the necessary measures to mitigate the effects; undertaking emergency prevention; organising the supply of the population with collective protection equipment; carrying out reconnaissance and mapping of the hazard area, rescue and other urgent operations; evaluate the people and property from risk territories; organise and restoration of disrupted critical infrastructure

services creating stockpile with essential supplies; making arrangements for the training for emergencies of chief officers, personnel, civil protection and rescue system forces and the population and investigate and analyse the causes of emergencies.

For the implementation of the goals and tasks the civil protection institutions have to be guided by the principles for the organisation and functioning of the system. The key principles include territorial, differentiation, compulsiveness, transparency, constant readiness and interoperability.

Civil protection and rescue system institutions are guided by the Constitution of Lithuania, laws and other legal acts enacted by the Parliament, decrees of the President of the Republic, Government Resolutions, Prime Minister's ordinances, orders of the National Defence Minister and international treaties to which Lithuania is a member.

Declaring and lifting emergencies is the responsibility of the government, which is also a charge when lifting a national level of emergency, establishing the procedure for organising rescue, search operations and urgent actions and responding to emergencies and mitigating their consequences. The government is in charge of evacuation measures as well as for shelters and other collective protection mechanisms in Lithuania.

The key duties and functions of the public administration and local government institutions as well as economic entities in the sphere of civil protection are as follows:

The Government is responsible for drawing up civil protection and rescue system development programmes and submitting them to the Parliament for approval; for developing the procedure for implementing civil protection and rescue system priority development trends; for establishing the emergency prevention procedure; approving the levels of civil protection preparedness, emergency criteria; approving national level plans of civil protection emergency preparedness; establishing the procedure for using the material resources in case of an emergency as well as the composition of state reserve technical means, food, clothing, the size of the reserve, etc.; preparing the civil protection training procedure; notifying the President and the Parliament about emergencies, their consequences and causes, and in support of the declaration of an emergency situation.

The Ministry of National Defence in peacetime has to implement, in cooperation with other institutions, the Government's policy in the area of civil protection, to coordinate the activities of civil protection and rescue system institutions in accomplishing the tasks assigned to their competence.

In addition, the Ministry of National Defence has the responsibility for specifying the procedure for notifying the Emergency Management Centre of emergencies; approving the needs for shelters and other collective protection structures, the norms and procedure of provision of the population with individual means of protection; approving the plans of the national level civil protection exercise and the annual plan for the enrolment of students in the civil protection training centre; approving the annual plan of activities of its Civil Protection Department; and presenting to the Government generalised information on the state of the civil protection and rescue system.

The Civil Protection Department is an essential part of the civil protection and rescue system, directing the activities of the civil protection and rescue system, organising the prevention of

emergencies, coordinating the activities of public institutions and economic entities in the sphere of civil protection and planning the national preparedness for the implementation of civil protection tasks in case of emergencies in time of peace and in wartime.

The tasks assigned to the Civil Protection Department include informing state institutions, economic entities and the population of a national-scale threat in case of an emergency; planning of measures to ensure the optimum use of state resources, localisation of emergency area and for mitigation of the effects of the crisis; compiling the register of objects of national significance which are potentially hazardous; controlling the activities of the civil protection and rescue system; organising the preparedness of public administration institutions and the community for actions in case of an emergency; and organising and directing the national level civil protection exercise.

The State Fire Prevention and Rescue Service is part of the Civil Protection and Rescue System maintaining constant readiness and commands for the extinguishing fires, search and rescue as well as providing first aid in emergencies. The State Fire Prevention and Rescue Service is subordinate to the Fire Prevention and Rescue Department under the Ministry of the Interior

The State Fire Prevention and Rescue Service carries out state supervision of fire prevention and its tasks include fire prevention and guaranteeing of the availability of technical and organisational measures for extinguishing fires. The work of state fire prevention supervision is organised in compliance with the regulations approved by the Government.

The activities of ministries and other institutions in the civil protection domain are directed by their chief executives or persons authorised by the chief executives. The most important tasks of ministries and other authorities include: organisation of civil protection according to the type of activity and competence assigned to them; approval of regulations of the emergency management centre of ministry or other institution of state administration, as well as plans of emergency preparedness upon coordination with the Civil Protection Department; building of departmental reserves of supplies and funds in order to increase the stability of functioning and security under emergency conditions; organisation of training in civil protection for the chief executives and experts; drawing up plans of emergency preparedness of civil protection; coordination of the planning of civil protection measures; and conducting a yearly analysis of the state of emergency preparedness of civil protection and submitting it to the Civil Protection Department.

The County Governor is the lead authority in civil protection of the county. Their responsibilities are defined by the Civil Protection Law²⁷.

The Mayor of a district or city has the following responsibilities for crises management: to be responsible for the preparedness of civil protection within the territory of the municipality; organization development of a plan of preparedness of civil protection in the event of emergencies; warn public authorities, economic entities and the population about the scope and possible effect of the emergency and others.

²⁷ More details about Governor's responsibilities see on p. 23 of the "Lithuania: Capabilities, Organisations, Policies, and Legislation in crisis management and disaster response", p.22 <https://isij.eu/article/lithuania-capabilities-organisations-policies-and-legislation-crisis-management-and-disaster>

Further, the Mayor has to implement preventive measures for civil protection, rescue and other urgent tasks, mitigate the effects of emergencies, evaluate the population and to organise civil protection training of the population²⁸.

Public organisations may be called to take part in organising state protection measures for elimination of the consequences of emergencies and to provide assistance to victims in cooperation with the municipal civil protection service units.

Institutions

At the Governmental level, the National Security Commission, established in 2017, deliberates and coordinates various national security matters, including strategic/policy issues related to civil preparedness, resilience, emergency situations and crisis management. The National Security Commission consists of the Prime Minister, Minister of Defence, Minister of Foreign Affairs, Minister of the Interior, Minister of Economy and Innovation, Advisor to the President, Director of State Security Department, Director of Second Investigations Department under the MOD, and Chancellor of the Government. The Threat Management and Crisis Prevention Bureau in the Government Office supports the National Security Commission and is also responsible for developing an integrated crisis management and hybrid threat prevention system, coordinating the implementation of the national crisis management procedures according to NATO and EU crisis management procedures, and coordinating state strategic communication in the field of national security.

Civil preparedness activities in Lithuania are implemented via the civil protection and partially through the mobilisation and host nation support (as much as it involves civilian support) system.

The Government of the Republic of Lithuania is responsible for civil protection policy making. The Minister of the Interior is in charge of drafting civil protection legislation, establishing the procedure for the exchange of information on emergencies, making proposals to the Government on the need for budget appropriations for the civil protection system and approving national level civil protection exercises plans. The Minister of the Interior also heads the Government Emergency Commission, which evaluates the state of civil protection system in Lithuania, makes proposals to the Government on improving civil protection and decides to activate the National Emergency Operations Centre.

The Fire and Rescue Department under the Ministry of the Interior coordinates the activities of institutions in the field of civil protection. It coordinates the execution of prevention of emergencies and the planning of preparedness for emergencies.

The Civil Protection and Rescue System of Lithuania is comprised of: the Government Emergency Commission; the Emergency Management Centre; the Civil Protection Department under the Ministry of National Defence; the State Fire Prevention and Rescue Service; and fire protection, search and rescue, other territorial population warning and information, evacuation and civil

²⁸ More responsibilities of Mayor are on p.23-24 of the "Lithuania: Capabilities, Organisations, Policies, and Legislation in crisis management and disaster response", p.22
<https://isij.eu/article/lithuania-capabilities-organisations-policies-and-legislation-crisis-management-and-disaster>

protection services of ministries, other institutions of public administration and local government municipalities, civil protection and rescue system bodies of economic entities; environment monitoring and laboratory control network.

The civil protection system of Lithuania is managed and organised at three levels: national, county and municipal. At national level, the key actors are the Government, the Government Emergency Commission, the Ministry of the Interior, the Fire and Rescue Department under the Ministry of the Interior and the subordinated agencies, ministries and other state institutions make strategic decisions regarding the implementation of civil protection measures.

At county level, the system is organised by county governors, county civil protection departments and county emergency management centres. At municipal level, municipal administrators, civil protection departments, civil protection personnel, municipal emergency management centres, fire prevention and other civil protection services, economic entities and agencies are responsible for the organisation of preparedness for emergencies and the respond to such events.

Departmental emergency management centres shall be established at the ministries and other public administration institutions. Emergency management centres shall be formed under the office of the county governor and the district (city) mayor. The regulations, heads and structure of these centres shall be approved by the founders. Permanent civil protection staff has to be employed at all the potentially hazardous facilities.

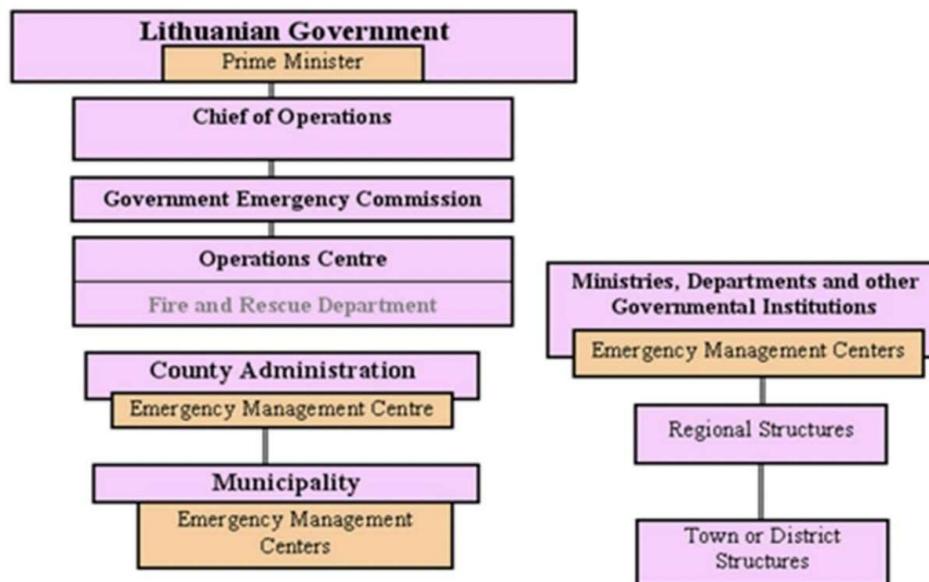


Figure 2. Organisational chart of the Lithuanian crisis management structure. (Source EC ECHO)

The Government Emergency Commission is a permanent Government commission responsible for organising emergency prevention and direct emergency relief actions in cases where an emergency

encompasses the territory of one or more counties or where there is a need for assistance from public administration bodies for rallying without delay forces and material resources necessary for mitigation of the effects an emergency.

The Emergency Management Centre is established to function as a permanent institution of the Emergency Commission having the function of a Government institution. In the event of large-scale natural disasters, technological accidents and catastrophes the Centre is responsible for organising disaster containment, rescue of people and mitigation of the effects.

In the event of emergencies the Emergency Management Centre has to adopt and submit to the ministries, other public administration institutions, local authorities and the population mandatory decisions on localisation and mitigation of the effects of an emergency. The Emergency Management Centre has to be established and its regulations approved by the Government.

The tasks of the Emergency Management Centre include performing monitoring of risk factors and threats, forecasting possible crises; coordinating activities of state institutions and entities within the crisis prevention area; ensuring the operation of crisis management infrastructure and constant exchange of information on crisis management between institutions; and developing international cooperation within the field of crisis management.

Further, the Centre, in implementing the tasks assigned to it, collects and analyses information received from the national authorities, mass communication and news agencies regarding threats and ensures the protection of information representing a state or official secret. The Centre carries out a comprehensive analysis of information received in the area of crisis management, forecasting possible crisis situations and the scope of such situations; prepares for the President, the Parliament, the Government and the Council of National Defence overviews of the most important developments, special communications and draft recommendations regarding crisis prevention.

The Centre acts as a contact point for the national authorities and international organisations that is available 24/7.



Figure 3. Lines of coordination of the Lithuanian crisis management system. (Source EC ECHO)

The tasks of the Emergency Management Centre include performing monitoring of risk factors and threats, forecasting possible crises; coordinating activities of state institutions and entities within the crisis prevention area; ensuring the operation of crisis management infrastructure and constant exchange of information on crisis management between institutions; and to develop international cooperation within the field of crisis management.

The Emergency Commissions are the main operational bodies of the civil security system in Lithuania and are technically assisted by the Fire and Rescue Service. There are two types of emergency commissions: at governmental and municipal levels.

The main operational bodies of the civil security system in Lithuania are the Emergency Commissions, which are technically assisted by the State Fire and Rescue Service. The emergency commissions can be formed on two levels: municipal, chaired by the director of municipal administration and government, chaired by the minister of Interior.

The role of the Fire and Rescue Department is to implement civil protection measures developed by the government and to coordinate the activities of governmental institutions and economic entities. In addition, the Department prepares civil protection plans for the management of emergencies, major accidents and natural disasters in both peacetime and wartime, as well as organises the training and education of emergency officers.

The National Emergency Management Plan defines the procedures for warning and informing the public, for rescue operations and coordination and for organising crisis communication, as well as the procedures for evacuation.

The National Emergency Management Plan defines the procedures for warning and informing the public, for rescue operations and coordination and for organising crisis communication, as well as the procedures for evacuation.

In addition, the Plan is a document that defines the material and human resources of the civil protection entities in event of municipal or state level emergencies, as well as the procedures for mobilisation of human resources and for the organisation of liquidation, elimination for the consequences thereof.

Disaster contingency plans of state level include:

- Plan of the Republic of Lithuania on population protection in case of a radiological accident at Ignalina Nuclear Power Plant,
- State search and rescue plan in case of an aircraft or watercraft accident in the territory of the Republic of Lithuania,
- National sea accidents pollution liquidation plan,
- State rescue and flood consequences liquidation in Klaipeda county plan.

The Minister of Interior approves the national civil protection exercises and is in charge of information exchange on an incident or emergency event.

The National Emergency Management Plan states the procedure for warning and informing the public, for rescue operations and coordination? Organisation of communication, the provisions of material resources and their use, as well as the procedures for evacuation.

The Fire and rescue Department is an essential institution of the Lithuania civil security system in directing the activities of the civil protection and for coordinating the overall national organisation of emergency prevention. The Fire and Rescue Department also has the main responsibility of early warning and public information in case of an emergency.

Lithuania has an early warning system for emergency situations. It is constantly operational and is fully automatic.

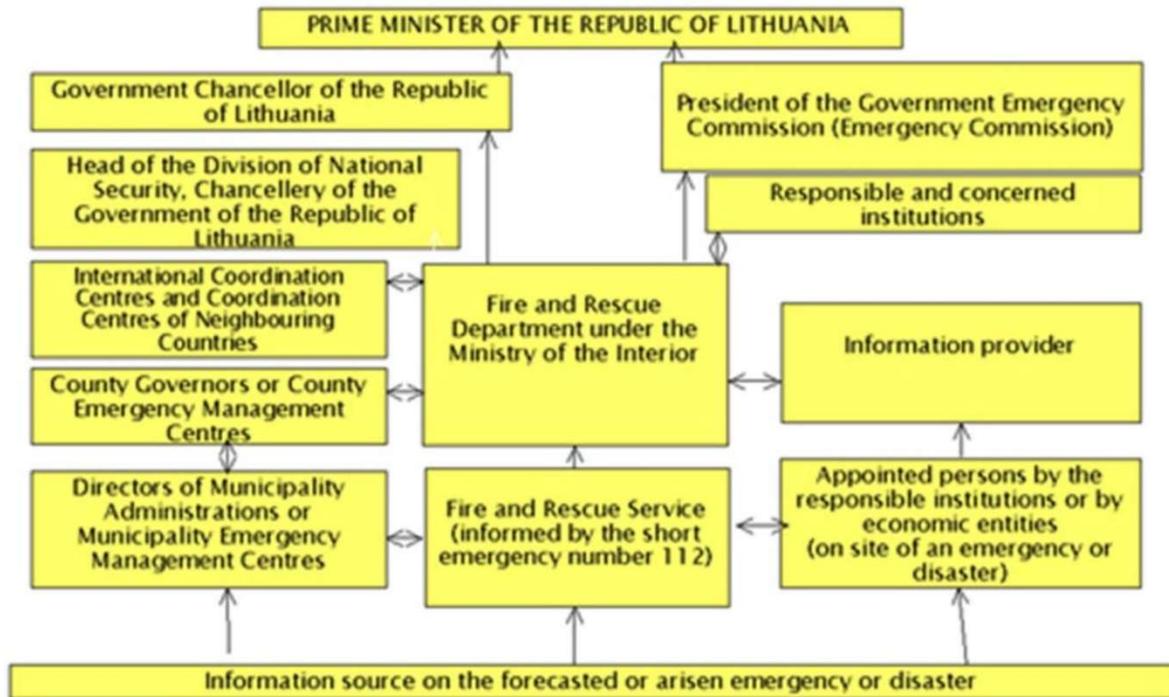


Figure 4. Lines of communication of the Lithuanian crisis management structure. (Source EC ECHO)

Training. In Lithuania the Minister of Interior approves the national civil protection exercises. Training in the basics of civil protection is organised in secondary schools and college education institutions through programmes developed by the Ministry of Education and Science.

The Civil Protection Training Centre is the principal educational authority for civil protection and rescue activities. The Training Centre is established and its regulations are approved by the Minister of National Defence.

Conclusion

The crisis management in Lithuania is oriented to be centralised, like in the other two Baltic states. The term “Resilience” is not used in Lithuanian policy or legislative documents. What is meant by “Resilience” is, in fact, a desired outcome from implementing the National Security Strategy that provides a vision of the state’s development, its national interests and the necessary actions for their implementation and the Civil Protection and Rescue System that guarantees the optimum use of state resources in order to ensure public security, maintain the operability of the national economy, localise the emergency areas and mitigate the effects thereof.

The new Crisis management and Civil protection law of the Republic of Lithuania provides for the concept of crisis management. “Crisis management - activities that include the prediction, monitoring, preparation and implementation of preventive and preparedness measures, the liquidation of crises and the removal of their consequences.” The law is planned to be adopted in the fall of 2022.

In 2020 the Government of Lithuania adopted the National Progress Plan for 2021–2030. Inter alia this plan establishes that adequate crisis preparedness is one of the most important elements in increasing the resilience of the state and society. One of the tasks of this plan is to ensure effective management of emergencies and national security crises.

In the Government Programme Implementation Plan for 2021–2023 the creation of an effective crisis and emergency management system is planned. Implementation of this measure will include the establishment of The National Crises and Emergencies Management Centre.

Latvia

Resilience

The national resilience system is integrated and is an integral part of a so-called comprehensive national defence (CND) system. The aim of CND is to strengthen the cooperation among state institutions, provide effective mechanisms for public - private partnership, increase the skills and capabilities of the society to protect themselves, in case of any crisis, military and non-military. Comprehensive defence comprises several pillars, part of which are related to resilience: Civil Defence, Economic resilience, Psychological resilience etc.

Legislation

1. Constitution of the Republic of Latvia²⁹;
2. The National Security Law³⁰;
3. The Civil Protection Law³¹;
4. Latvia: Capabilities, Organisations, Policies, and Legislation in crisis management and disaster response³²

Latvia has introduced a similar concept as many Scandinavian nations - to focus on continuity of essential services during any disaster. As a result, all essential service providers are tasked to establish business continuity systems for all disasters and even the war.

In short, the Latvian comprehensive national defence system heavily depends on the resilience of society, essential service providers and key institutions. There is a formal structure to coordinate all efforts led by the MoD. Resilience tasks are included in formal planning documents, and each institution has clear tasks (wartime tasks). The essential personnel are identified and have wartime tasks (obligation to work). MoD is also responsible for cyber security, and similarly, all resilience tasks for IT systems, hardware and software are set by the MoD.

²⁹ https://www.constituteproject.org/constitution/Latvia_201

³⁰ <https://investmentpolicy.unctad.org/investment>

³¹ <http://connections-qj.org/article/latvia-capabilities-organisations-poli>

³² <http://connections-qj.org/article/latvia-cap>

It's important to highlight that in Latvia, resilience activities are defence-driven, and part of resilience activities is also resistance planning³³.

The National Security Concept is a strategic document based on analysis of national threat stating principles for prevention of threats, priorities and measures, which must be taken into account when executing new political planning documents, legislative enactments and action plans in the area of national security. The document is prepared by the Latvian Cabinet, examined by the National Security Council and approved by the Parliament, at least once on each convening (by 1 October) from its first year of operation.

The Concept sets out that disasters listed in the National Civil Security Plan, such as storms, extreme temperatures, earthquakes, floods, fires, leakage of dangerous substances, industrial accidents, dangerous infectious diseases, etc., must be resolved within the framework of the civil security system. The priorities determined in the Concept provide the basis for the development of the National Security Plan by the Cabinet of Ministers. The Plan includes specific state threat neutralisation and prevention measures and means.

In order to ensure the forecast of potential crises, timely decision-making and implementation of measures for management and coordination of state and municipal institutions in preventing crisis situations and mitigating the consequences, the national crisis management system is being developed and enhanced.

The National Security Law determines the national security system and tasks of such, the competence of the persons or institutions responsible for the national security system and the principles and procedures of coordination, implementation and control of their activities.

According to it, the Crisis Management Council in case of a danger to the State coordinates civil-military cooperation and the operational measures of national administration institutions in suppression of the danger to the State. The by-law of the Crisis Management Council shall be approved by the Cabinet. The Crisis Management Council is chaired by the Prime Minister and it is composed of the Ministers for the Interior, for Defence, for Foreign Affairs, for Economics, for Finance, for Justice and for Health. The Council may include the heads of State security institutions as well as other State officials but with advisory rights.

The competence of the Crisis Management Council includes coordination of the operational management for suppression of the emergency; to coordinate the development of plans for the prevention of danger to the State; and to prepare for submission to the Cabinet proposals regarding the specification of national security system emergency preparedness. Additionally, in the case of a danger to the State, the Council coordinates the unified and timely implementation of political decisions in national administration institutions, prepares and submits to the Cabinet proposals regarding the status of critically important infrastructure for the national security, alongside the security measures that need to be performed.

The Crisis Management Council is supported by the Crisis Management Secretariat which guarantees the operation of the Council and ensures the purposeful and continuous provision of cooperation and support of the responsible institutions to the Crisis Management Council.

The National Security Law also defines the provisions for the State Civil Protection Plan, which has to be drawn up by the Ministry of the Interior in cooperation with other ministries and approved by the Cabinet. The State Civil Protection Plan incorporates the measures for the implementation of the State civil protection system, as well as measures for preventive, readiness and response actions intended in states of emergency, as well as the measures for liquidation of consequences of such events.

³³ <https://www.securebaltics.eu/resilience-as-the-first-line-of-defence/>

The Civil Protection Law is the other main legislative document in Latvia which provides the Structure and Organisation of the civil protection system. The purpose of the act is to create a system of civil protection for disaster management, ensuring the legal and organisational grounds for the protection of persons, property and the environment in cases of disasters and when there are threats of disaster.

It defines that the structure of the civil protection system has to be formed by the national institutions, local governments and merchants. The main tasks of the system are to carry out disaster management; to provide aid to victims of disasters; to reduce the possible damage to property and the environment caused by disasters; and in emergency situations caused by military invasion or war to support the National Armed Forces with resources.

The Civil Protection Law also defines the management procedures of the civil protection system. The Prime Minister has the responsibility for the operation of the system and the implementation of the tasks thereof and, within the framework of the system, to manage the measures at national or regional level for the prevention and overcoming the emergency situation.

The State Firefighting and Rescue Service shall manage, coordinate and control the operation of the system, however depending on the type of disaster the emergency measures for the response and elimination of the consequences may be taken by another competent national institution indicated in the State civil protection plan or the local government civil protection plans.

According to the National Security Law the Cabinet has the responsibility to announce a state of emergency, exceptional state and mobilisation in cases determined by law, as well as to decide upon the necessity for support by the armed forces of the North Atlantic Treaty Organisation and European Union Member States during a state of emergency or exceptional state. In addition, the Cabinet has the responsibility for strengthening the national defence capacity in peace time.

An exceptional state has to be declared in the cases in which the state is endangered by an external enemy or within the country internal disturbances have occurred, or if there is a threat that such may arise, in this way endangering the nation. In cases of a state of emergency and exceptional state, mobilisation may be announced in order to carry out tasks related to national security and national defence, as well as to liquidate consequences

The Civil Protection Law defines the tasks of the state institutions and ministries in civil protection which include exploring possible threats in the sector and submitting proposals to the Ministry of Interior up to 20 January each year regarding the clarification of the national civil protection plan, as well as notifying regarding the measures and operations carried out in civil protection during the previous year.

In addition, ministries need to plan action for the provision of the operation of the sector in cases of disaster, to coordinate the operation of the subordinated authorities in cases of disasters and coordinate and control the formation of the State material reserves in the sector.

According to this legislative act the Cabinet defines the procedures by which institutions, organisations and commercial companies have to establish fire safety, firefighting and rescue services; and subsequent functions and rights.

At the local level the Civil Protection Law describes the tasks and rights of local governments in civil protection. The emphasis is on the role of the chairperson of the local government city or county council, who holds the responsibility for the implementation of the tasks for civil protection in the relevant administrative territory. The main tasks of the local governments include establishing and managing the district civil protection commission; participating in preventive measures in the relevant administrative territory; providing support for operation and emergency services and if necessary, to evacuate the inhabitants from the territories endangered or affected by a disaster. The

civil protection commission of the local government operates pursuant to the regulations developed in accordance with the model regulations approved by the Cabinet.

Institutions

The Ministry of Defence is responsible for the coordination of the implementation of comprehensive national defence and resilience tasks in all sectors. In the middle of 2022, a new state secretary's level working group was established to formalise the interagency coordination (previous one group was established in 2018). Each ministry has formal tasks to implement sectoral resilience guidelines. Part of resilience tasks have to be implemented by the municipalities (as a part of civil protection plans) - prepare to accommodate IDPs, create shelters etc.

The Ministry of Defence is leading a working group of state secretaries (or their deputies) overseeing the implementation of comprehensive national defence. Their task is to supervise the work of the seven thematic subgroups, as well as to propose to them the issues and tasks to be solved for the future implementation of comprehensive national defence. The thematic subgroups are led by the responsible sector ministries, and consists of their subordinate institutions, sector regulators, representatives of critical infrastructure, vital service providers and non-governmental organisations, in order to ensure comprehensive development of the subgroup's range of issues to promote and ensure resilience and continuity of various military and non-military nature in cases of crisis. But the implementation is decentralised, as every institution is responsible for their own resilience and the resilience of their sector³⁴.

The overall responsibility for crisis management and for the continuous function of the operation of the civil protection system lies with the Prime Minister of Latvia. Civil protection operations are planned, coordinated, and led by the State Fire and Rescue Service - an organisation subordinated to the Ministry of the Interior, while the heads of institutions and companies are responsible for civil protection in their own institutions and companies.

The Prime Minister leads the Crisis Management Council which is the main managing body in the emergency events. The Crisis Management Council coordinates the operational measures of the involved national institutions in events of disasters and in cases of civil-military cooperation. The Crisis Management Council Secretariat supports the activities and guarantees the successful functioning of the Council.

The State Fire and Rescue Service performs and manages firefighting and rescue operations and activities, responds, performs and manages rescue operations in road accidents and fires, as well as performs rescue works in water accidents. The functions of the State Fire and Rescue Service include implementing state policy in the field of fire safety, firefighting, civil protection and operation of the single emergency phone number 112. The State Fire and Rescue Service in cooperation with local governments develops emergency plans for the provision of prevention, preparedness, response and recovery in emergency measures, taking into account the potential types of disasters, the scale and high-risk subjects in the administrative area.

At the local level the municipal authorities are responsible for establishing and managing the Civil Protection Commission of the municipalities and cities under state jurisdiction. The Commission coordinates civil protection measures in disaster events in the relevant local administrative territories.

³⁴ <https://www.sargs.lv/lv/hozares-politika/2022-06-01/izveido-darba-grupu-visaptverosas-valsts-aizsardzibas-ieviesanas>

The civil protection framework of Latvia foresees the involvement of military forces to civil authorities during peacetime emergencies. The structure of the National Armed Forces consists of the Defence Forces, the Home Guard and the Reserve Forces. Among the duties of the Armed Forces defined in the Armed Forces Law is the participation during peacetime emergency operations. Their main tasks include supporting civilian services with manpower, vehicles, communication and life-support equipment, participating in rescue work and in maintaining public order, as well as to fulfil other specific tasks that require their capabilities, such as blowing up ice on rivers, clearing mines, decontamination, etc.

The Home Guard is an organisation created on territorial principle in order to have a battalion ready within the territory of a district or city municipality. The Home Guard battalions have agreements concerning mutual assistance and cooperation with respective local and municipal fire brigades and police departments.⁸⁸ The largest emergency assistance operations carried out so far by the National Armed Forces have been the involvement in the forest fires of 1992 and the spring floods of 1996 and 1998.

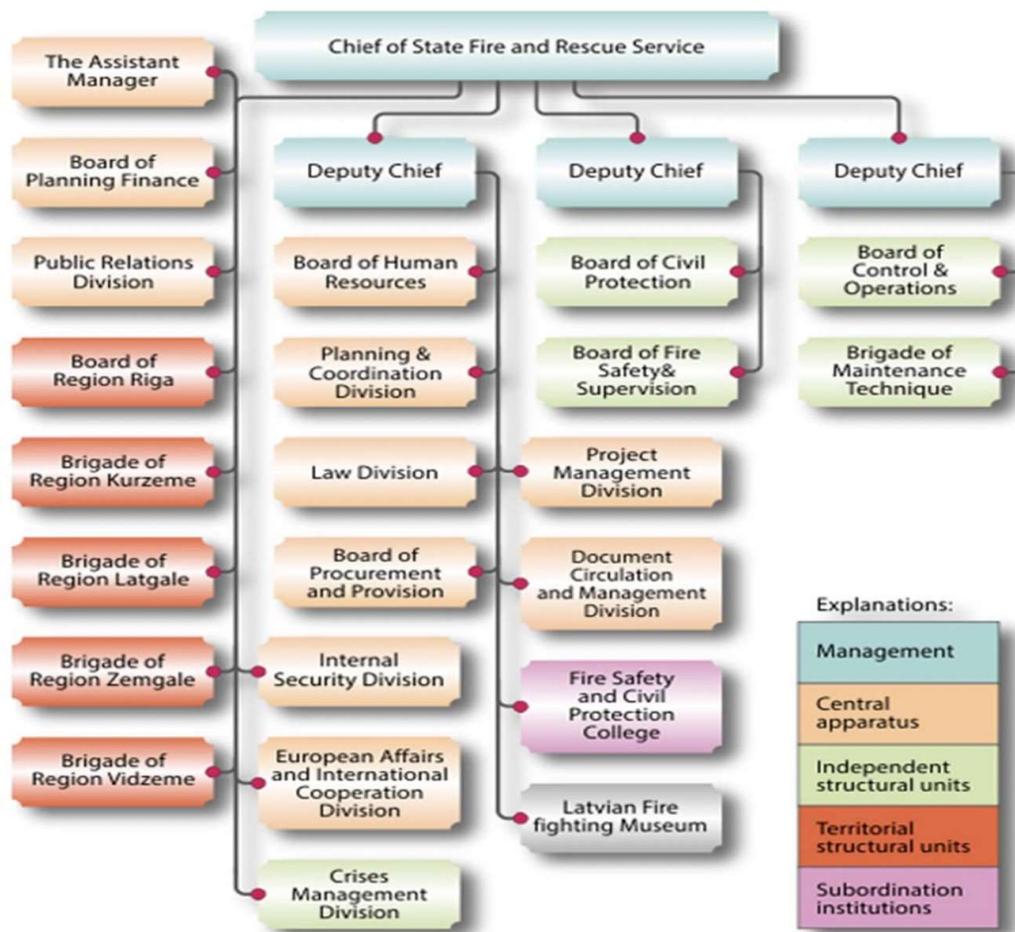


Figure 2. Structure of the State Fire and Rescue Service⁹⁰

Operational crisis management responsibility normally rests with the counties and municipalities which, after declaring a state of emergency, form task forces led by the highest local political actor. The overall coordinating responsibility for civil security in Latvia lies with the Ministry of Interior. It provides assistance at the local level along with others responsible for crisis management agencies.

To be more specific, operational cooperation in crisis management operations in Latvia could be divided into two main levels of responsibility – the national level and the institutional level (where ministries and their subordinate agencies are the main operational actors).

The national level is the highest level in the Latvian civil security system and is coordinated by the Crisis Management Council. The council has a coordination function as it coordinates operational crisis management between institutions and civil-military cooperation in events of disaster and other threats to the state. The Crisis Management Council is convened only in cases of major emergency, if the crisis is multi-sectoral and requires coordination.

The Council is chaired by the Prime Minister and is composed of other Ministers, as it coordinates the implementation of political decisions in emergency situations concerning national security. In addition it also coordinates the development of preventive plans.

The main operational crisis management is the second level of institutional responsibilities which is covered by the Ministries and agencies. The most important tasks of the ministries within the civil security system include the forecasting and prevention of possible threats in their sector, coordination and control of the operational response, to implement the State Civil Protection Plan and to maintain and further enhance the capacities for response and mitigation. Ministries also have to prepare action plans and coordinate the role of their subordinated bodies in emergency scenarios.

As one of subordinated organisations to the Ministry of Interior, the State Fire and Rescue Service is the main operational manager and coordinator for civil emergencies such as floods, fires, accidents, etc. Each ministry has several subordinated agencies directly or indirectly engaged in civil security issues.

Further, the Ministry of Interior coordinates several other agencies that include the State Emergency Medical Service, as the provider of health services in case of general public health emergencies; the Centre for Disease Prevention and Control, as the main responsible body in case of threats caused by diseases; the Security Police, as the main actor in events such as terrorist attacks; and the Coast Guard Service, which is the main actor in case of marine pollution and for search and rescue works at the sea.

Cross-border and international collaboration is also organised through the Monitoring and Information Centre (MIC), which is operated by the European Commission within the Framework of Community Mechanism to facilitate reinforced cooperation in civil protection assistance interventions and the Euro-Atlantic Disaster Response Coordination Centre.

The National Civil Protection Plan provides the provisions for civil protection entities undertaking preventive, preparedness, response and recovery emergency measures in occurrence of national and regional disasters, as well as a military invasion or in case of war. The Plan defines the implementation of the Civil Protection Law requirements and identifies the civil defence planning and operational objectives. Additionally, the document sets out the courses of action, tasks and the objectives in planning and carrying out civil protection measures in disaster events.

At local level Cabinet of Ministers Regulation No. 423 dated 26 June 2007 establishes the civil protection plans of local governments, merchants and institutions as well as the procedures for developing and approving these plans. In addition, there are several other Cabinet Regulations that provide for risk reduction measures such as No. 532 "Regulations regarding the procedures for industrial accident risk assessment and risk reduction measures" (19 July 2005) and No. 626 "Regulations regarding criteria for the specification of objects of increased danger and the duties of the owners (possessors, managers) of such objects for ensuring measures for reduction of risk" (18 September 2007).

Local governments develop the respective civil protection plans at local government level in cooperation with the State Fire and Rescue Service. Each civil security institution in Latvia has their specific crisis management procedure.

The Ministry of Interior coordinates the emergency logistics. The Latvian armed forces provide assistance in civilian emergencies in terms of manpower and logistics when required.

According to the Civil Protection Law the civil alarm and notification system has to ensure the warning and informing of the population regarding disasters or threats, as well as the announcement of an emergency situation, the state of emergency or mobilisation. The relevant procedures for the use, establishment and financing of the civil alarm and notification system are determined by the Latvian government. Mass media has to provide information received by the

State Fire and Rescue Service regarding the threat and guidance for further actions of the population free of charge in such an event.

The Crisis Communication Action Plan 2011 – 2013 is designed to provide planned, coherent and coordinated communications in crisis situations and to facilitate competence of the officials involved in communication as well as to raise awareness and educate the population for actions in the event of a crisis. The Plan also foresees the development of planned, integrated and coordinated public administration procedures for circulation of information in crisis situations. In addition, crisis communications expert group is to be established within the Crisis Management Council. The plan anticipates the development of recommendations for crisis communication intended for government communications professionals and other officials involved in crisis communications. Moreover, the development of procedures for managing crisis events information, as well as the rights and obligations of communications officers in crisis situations are stated in the Plan.

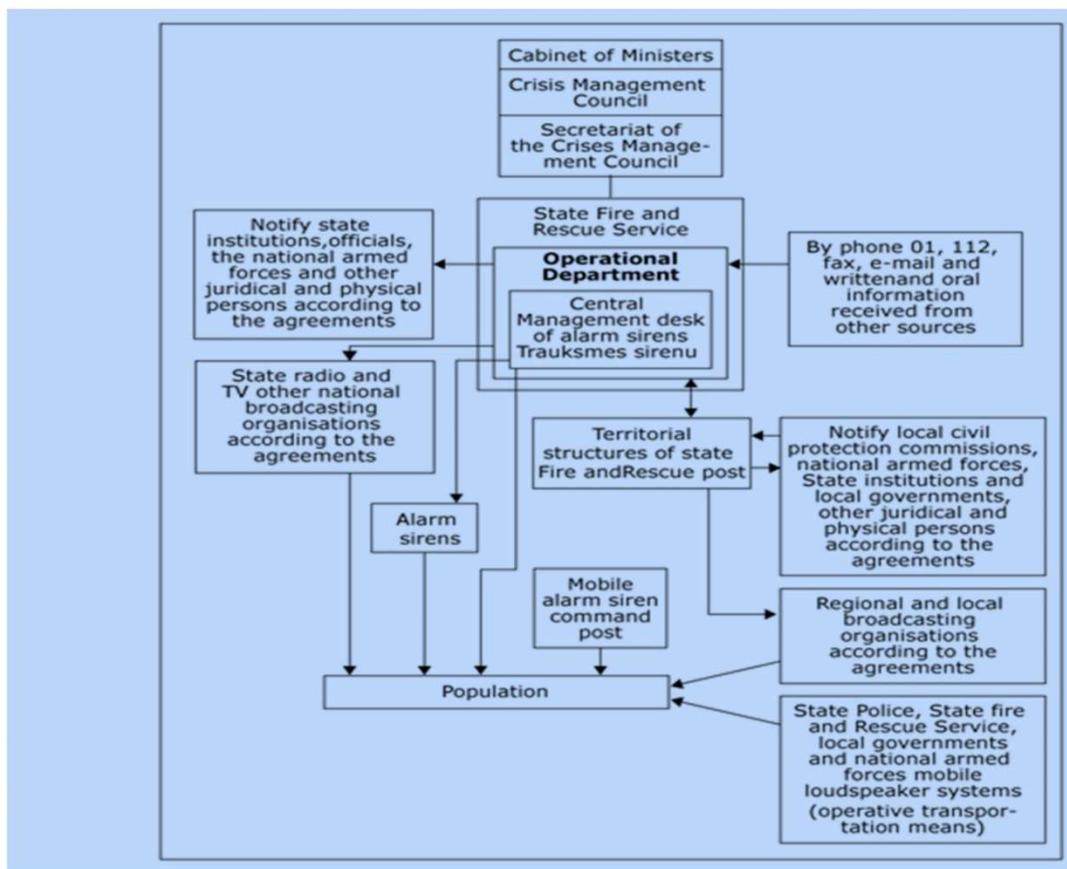


Figure 3. Civil alarm and notification system (Source: EC ECHO)

The Crisis Communication Action Plan highlights the importance of educational activities and actions in case of crisis situations. Existing training programs in secondary and vocational education institutions are to be updated and supplemented in order to increase the crisis communication knowledge of the state and local officials responsible in crises situations. Training of state and local government officials is also listed as one of the main tasks in the Plan for the developing efficient crisis communication. The Ministry of Interior is the coordinating authority for executing the plan.

Municipalities and local governments are main actors responsible for maintaining the emergency communication system. Emergency services in Latvia have their own risk mapping services including risk registration systems.

The “112” single emergency number has been implemented in Latvia and National Geographical Information Systems (GIS) is being gradually enhanced. The GIS system aims at describing the coordination of GIS services, collection of data and creation of state GIS portal. The aim of the GIS Pilot Project is to create a digital map of Riga with the information regarding emergency events that fall under the competence of the State Police and State Fire and Rescue Service. The overall responsibility and coordination for the development of GIS services has the Information Centre of the Ministry of Interior and the State Fire and Rescue Service. Additionally, the Electronic Communications Office has been established with its operational goal to manage the resources of radio-frequency range in the field of electronic communications.

Conclusions

The term “Resilience” is not widely in use in relation to civil protection or crisis management. Within the framework of this document resilience term has been identified in few research papers related to different topics. However, these topics do not cover civil protection or crisis management.

Like in the other two Baltic states, the Latvian CM system is centralised, i.e. it represents a strict top-down structure controlled by the central national civil protection authority.

The Prime Minister has the responsibility for the continuous function of the operation of the crisis management system and for the implementation of the related tasks and obligations. The State Fire and Rescue Service, an organisation directly subordinated to the Ministry of Interior, plans, coordinates, leads and controls the civil protection operations. The State Fire and Rescue Service has significant responsibility for crisis management at national level.

At the local level the municipal authorities are responsible for establishing and managing the Civil Protection Commission of the municipalities and cities. The Commission coordinates civil protection measures in crisis situations in their respective administrative territories. The civil protection framework of Latvia foresees the involvement of military forces in support of civil authorities during peacetime emergencies. Latvian Ministry of Foreign Affairs is responsible for the cooperation with the European Union as it implements and coordinates the state external security policy. Cross-border and international collaboration is also organised through the Monitoring and Information Centre operated by the European Commission.

Poland

Resilience

Resilience is a relatively new concept for Poland. After years of predominantly applying the concept of resilience in the field of preventing the devastating consequences of natural disasters and economic crises, the concept of resilience was introduced into the legal field in *the National Security Strategy*³⁵ in 2020. As part of further activities regarding the security of the state and its citizens, the

³⁵ https://www.bbn.gov.pl/ftp/dokumenty/National_Security_Strategy_of_the_Republic_of_Poland_2020.pdf

Strategy focuses on state defence and common defence.³⁶ It asserts that it is necessary to increase the state's resilience to threats by creating a system of common civil defence, based on the efforts of the entire nation, and building an understanding for the development of the Republic of Poland's resilience and defence capabilities. It places special emphasis on building a system of common civil defence and resilience to threats, including hybrid threats, through ensuring the universal nature of civil defence and the protection of the population.

The strategy sees it necessary to develop the capacity of the health system and public administration structures to fight against epidemic threats, especially against highly infectious and particularly dangerous diseases. As noted, it is also necessary to develop diagnostic facilities and the strategic reserve programme.

The document describes plans of increasing resilience to threats by ensuring effective energy supplies, preventing the uncontrolled movement of people and the relocation of the population, and the collection, protection, and management of food and water resources.

The strategy recognises the need for the transfer of know-how and capacities allowing the shaping of national security, based on the broad involvement of public authorities, including local government, educational, higher educational and scientific institutions, and the economy. It approaches building social capital by developing cooperation skills, networks of formal and non-formal social organisations, and by shaping the community of values within Polish society.

Strategy identifies the need to redefine the civil defence system and the population-protection system by making it universal, and to develop a law comprehensively regulating the subject matter of civil defence. The document expresses the need to develop the state's capacity to prevent and respond to terrorist threats and to fight organised crime, including criminal activities in cyberspace.

A lot of attention is paid to cybersecurity. It was determined to increase resilience and information protection levels in the military sector, while promoting practices enabling citizens to better protect their information. Further goals include the creation of resilient telecommunication networks and Information and Communications Technology systems, population information and alert systems, and resilient transport networks. This is associated with the assumption of implementing a homogeneous system of human resources management, including the administration of personnel reserves.

The strategy also indicates the need to strengthen legal certainty by ensuring effective legal protection for citizens, an efficient judiciary system, and the proper enforcement of court decisions. The need to continue strengthening the counter-intelligence protection of the state authorities and critical infrastructure in a way commensurate with increasing activities of foreign intelligence services, in both the military and civilian domains, is noted. The strategy states that it is crucial to develop the capacities of national intelligence services to identify risks at an early stage.

The strategy noted the need for strengthening interagency coordination with a view to developing the capabilities of the national industrial and technological defence base within state security, including the selective launching of actions to mobilise the economy, and to meet the needs of the Polish Armed Forces. Finally, the document identifies the need to increase capabilities in the fields of cryptology and the production of telecommunication appliances equipped with cryptographic modules, and to build capacities for technological development and the production of strategic resources in times of peace, crisis and war.

³⁶ https://link.springer.com/content/pdf/10.1007/978-3-030-78551-2_8.pdf

Another issue is the need to strengthen the Polish Armed Forces and their operational capabilities. The strategy assumes efforts to increase the growth rate of defence spending, to reach 2.5% of GDP in 2024. It points to the necessity of continuing the adaptation of the command structure of the Polish Armed Forces to reflect the needs resulting from changes in the security environment. It also describes it as vital to supplement the personnel and equipment of the Armed Forces, and to adapt training programmes and capabilities to conduct asymmetric operations. It provides for enhancing the mobility of troops and the efficiency of their support and logistics systems.

Strengthening the capabilities of the North Atlantic Treaty Organisation and the European Union is considered necessary. The document declares that divisions among European Union Member States should be prevented. Within this pillar, the strategy also discussed the need to develop cooperation in bilateral, regional, and global formats, including with the United States and key European partners. It also raises the need to take steps to enhance the effectiveness of the United Nations and the Organization for Security and Co-operation in Europe. It stresses that national interests will be pursued in the spirit of solidarity with allies and partners.

The document emphasises the need to strengthen national identity, rooted in the Christian heritage and universal values. It highlights the notions of shaping and developing patriotic attitudes, refining instruments and procedures for the protection of cultural heritage, and promoting the development and protection of traditional family values, Polish national identity, language, culture, science, history and traditions. It promises to strengthen the links between the Polish diaspora and the homecountry.

Another objective established is strengthening the “brand” of the Polish economy and to support Polish companies in the process of internationalisation.

Also, the strategy holds as fundamental that steps should be taken to improve the conditions for the protection and development of families, and to increase the health security of citizens. It also identifies the need to take measures to improve the demographic situation, including an increase in the birth rate. Finally, the authors consider it essential to continue to develop physical culture, by ensuring universal access to sport, and by modernising the existing sports and leisure infrastructure, and constructing new facilities.

Another tangential application of the concept of resilience is *the National Recovery and Resilience Plan* within the framework of the EU program for restoring the economy after the crisis related to the coronavirus pandemic.³⁷ However, its scope extends beyond compensating for losses caused by the pandemic. It aims primarily to introduce reforms enabling the establishment of a digital and green economy, resilient to shocks and potential future crises.

The aims of the National Recovery and Resilience Plan include:

- strengthening the potential for economic growth,
- creating jobs,
- increasing the economic and social resilience of the state,
- offsetting the effects of the economic and social crisis,
- strengthening economic, social and territorial cohesion.

The National Recovery and Resilience Plan will include reforms and public investments in the following areas:

³⁷ <https://www.gov.pl/web/development-technologv/the-national-recovery-and-resilience-plan-amounts-to-approximately-60-billion-for-poland>

- public finances,
- health care reform,
- the labour market,
- innovations,
- qualifications,
- investment policy,
- business environment,
- education,
- infrastructure,
- transport
- new technologies,
- energy,
- buildings.

The website available at planodbudowy.gov.pl allows any interested citizen to submit their idea in one of the four areas recognised by the Ministry of Economic Development as a priority of the works related to the National Recovery and Resilience Plan. They include:

- Resilient society
- Resistant country
- Resilient environment
- Resilient economy

Legislation

So, as early as 2013, in the White Paper of National Security, resilience is mentioned only once in the context of crisis infrastructure security. But already in the National Security Strategy, adopted in 2020, a whole section Resilience of the state and common civic defence is devoted to the issue of resilience. In addition, the concept of resilience is mentioned in the Cyber Security, Economic Security and Energy Security sections. However, the Law on the Protection of the Fatherland, adopted in March 2022, still does not mention national resilience.

Instead, issues of economic resilience are widely presented in the context of the Covid-19 pandemic within the framework of the European Union program. The Ministry of Economic Development has prepared projects for the National Recovery and Resilience Plan in the following areas: innovation, digitization, green economy, circular economy, energy, thermal upgrading. The measures under the programme are intended to strengthen our social and economic resilience to future challenges and crises.

List of legislative acts:

- National Security Strategy³⁸

³⁸ https://www.bbn.gov.pl/ftp/dokumenty/National_Security_Strategy_of_the_Republic_of_Poland_2020.pdf

- Act on Crisis Management³⁹
- Law on the Protection of the Fatherland⁴⁰
- Regulatory and legal acts on territorial defence⁴¹
- The Cybersecurity Strategy of the Republic of Poland⁴²
- National crisis management plan⁴³
- National program for the protection of critical infrastructure⁴⁴

Institutions

Civil protection, Crisis management and Resilience issues are closely related. While the concept of national stability is just beginning to enter the Political and Legal State Architecture of the National Security system of the Republic of Poland, the crisis management system and the Civil Protection has a long tradition and can be considered fully formed.⁴⁵ In the absence of the law on Civil Protection, the Act on Crisis Management defines the activity of public administration bodies as part of the national security management, which consists of prevention of crisis situations, preparation for taking control over them by means of planned actions, reaction in the event of a crisis, removal of its effects, as well as restoration of resources and critical infrastructure.

Table 1. The structure of crisis management in Poland.⁴⁶

Administrative Level	Crisis Management Authority	Opinion Forming and Advisory Body	Crisis Management Office
National	Council of Ministers, Prime Minister	Government Crisis Management Team (RZZK)	Government Center for Security (RCB)
Ministerial	Minister in charge of government administration department	Ministerial Crisis Management Team	Ministerial Crisis Management Center
Province/Voivodship	Voivod	Voivodship Crisis Management Team (WZZK)	Voivodship Crisis Management Center (WCZK)
District	District (Foreman)	District Crisis Management Team (PZZK)	District Crisis Management Center (PCZK)
Communal	Community (Mayor)	Communal Crisis Management Team (GZZK)	Communal Crisis Management Center (GCZK) (optional)

³⁹ <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20070890590/U/D20070590L.j.pdf>

⁴⁰ <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20220000655/T/D20220655L.pdf>

⁴¹ <https://www.gov.pl/web/obrona-narodowa/akty-prawne>

⁴² <https://www.gov.pl/attachment/6a4aafc6-e339-4cd5-a8e6-cd47257f02d8>

⁴³ <https://rcb.gov.pl/krajowy-plan-zarzadzania-kryzysowego>

⁴⁴ <https://rcb.gov.pl/narodowy-program-ochrony-infrastruktury-krytycznej-2>

⁴⁵ <https://portal.cor.europa.eu/divisionpowers/Pages/Poland-Civil-protection.aspx>

⁴⁶ <https://www.sciencegate.app/document/10.3390/en14248286>, page 7

Institutions responsible for Civil Protection and Crisis Management⁴⁷

Central level

The Council of Ministers is responsible for:

- Maintaining public order;
- Internal security;
- Declaring the state of emergency.

The Ministry of the Interior and Administration is responsible for:

- General interior security with respect to criminal acts or natural catastrophes;
- Civil defence and crisis management;
- Search and rescue, oversight of ambulance services;
- Overseeing law enforcement agencies: the police, the Border Guard, the State Fire Service, and the State Security Service (Służba Ochrony Państwa).

The Ministry of Digitization is responsible for:

- Supervising and coordinating the actions of the government administration in crisis management;
- Allocating funds to help the victims of disasters; and
- Computerization of emergency systems to improve and accelerate rescue actions and assistance.

The Government Centre for Security (Rządowe Centrum Bezpieczeństwa) is a state budget unit (a Crisis Management Centre) subordinate to the Prime Minister is in charge of:

- Monitoring potential threats;
- Agreeing ministerial crisis management plans;
- Emergency preparation;
- Assessing emergency preparedness;
- Coordination of information during a crisis situation;
- Cooperating with external organisational entities, sections and units of international organisations in charge of crisis management and protection of critical infrastructure;
- Conducting trainings and exercises and participating in national and international exercises;
- Coordinating crisis and emergency management efforts.

The Government Crisis Management Team - Rządowy Zespół Zarządzania Kryzysowego, an advisory body, is responsible for:

- Initiating and coordinating activities related to crisis management;
- National Headquarters of the State Fire Service;
- Crisis management centres (*Centra Zarządzania Kryzysowego*).

⁴⁷ <https://portal.cor.europa.eu/divisionpowers/Pages/Poland-Civil-protection.aspx>

Regional level

Regional authorities are responsible for:

- *Voivodship* Emergency Response Board;
- *Voivodship* crisis management plan, in accordance with national guidelines;
- *Voivodship* crisis management centres;
- Managing the monitoring, planning, response and removal of the results of the threats on the territory of the *voivodship*;
- Performing civil security and civil planning tasks;
- Managing the organisation and delivery of exercises and training on crisis management;
- Assist lower governmental levels if their resources are inadequate;
- Supervise planning and response on county and municipal levels;
- Counteracting, preventing and removing the terrorism effects;
- Implementing critical infrastructure protection tasks.

Intermediate level

County authorities are responsible for:

- *Powiat* Emergency Response Board;
- *Powiat* crisis management plan;
- *Powiat* Crisis Management Centres;
- Civil protection;
- Fire protection;
- Management of monitoring, planning, response and removal of the consequences of the threats on the *powiat* territory;
- Performance of civil planning tasks.

Local level

Local authorities are responsible for:

- *Gmina* Emergency Response Board;
- *Gmina* Emergency Response Center
- *Gmina* crisis management plan;
- All local public issues relating to civil protection;
- Fire protection;
- Maintaining public order;
- Monitoring of threats;

- Early warning systems;
- Alarms;
- Coordinating rescue operations and evacuations;
- The mayor defines the civil protection tasks for all municipal institutions.
- National defence tasks (including keeping a register of pre-recruits, conduct defence exercises and trainings, planning and preparation of medical cover for defence needs, keeping control of subordinate units in this area, etc.).

Conclusions

Based on the results of a cabinet research, it seems that Poland is only beginning work on bringing the activities of state institutions to coordinated multi-sectoral interaction within the framework of the National Resilience (Resilience of State) system.

The concept of sectoral, state and social resilience has not yet become unifying in the formation of national and sectoral policies. In particular, there are generally no publicly available documents detailing the sectoral resilience elements mentioned in the National Security Strategy of the Republic of Poland approved on May 12, 2020. The strategy is the most important document on security and defence and is the basis for the development of more detailed documents such as the political and strategic defence directive.

References to resilience have already been included in the Strategy, which indicates that the issue of building resilience has become very important in the context of consolidating national security. Already in the introduction to the Strategy, in the description of the security environment, there are references to the need to increase the resilience of the state and society. They were developed in the chapter entitled State immunity and universal defence.

Some resilience-related elements are included in the National Crisis Management Plan and the National Critical Infrastructure Protection Program.

Within the framework of the European Union, work is underway to coordinate the actions of Member States for the resilience of states and societies against hybrid and cyber threats that may disrupt critical infrastructure. The process of adopting European Council Conclusions on strengthening resilience and combating hybrid threats in the context of the COVID-19 crisis is ongoing. They take into account issues related to "societal resilience". The Union also recognizes the need to build resilience beyond Member States' borders - on the principle that the more resilient neighbors, the more secure the Union. The EU also cooperates with NATO, which is of great importance for increasing the level of security on the continent.⁴⁸

The absence of a developed National Resilience system does not prevent the Polish authorities from making correct and timely decisions, which as a result strengthen state and social resilience. Among such successful decisions in recent years, two can be noted. The first is finding alternative sources of energy raw materials and creating additional routes for their supply. The second is the strengthening of territorial defence forces.

⁴⁸ <https://www.gov.pl/web/rcb/spoleczenstwo-odporne-na-zagrozenia>

It is appropriate to note the following factors that contributed to the achievement of positive results in the governance practice of Poland regarding the management of the development of the national security system:

- a high level of awareness of national identity, social unity and solidarity;
- constancy and consistency of the foreign and military-political course for joining NATO and the EU in the conditions of a dynamic security environment;
- high level of adaptability of the national security system to sudden and drastic changes in the security environment due to the high level of institutional capacity of the relevant state bodies.

But despite generally effective and capable state institutions, the architecture of the security system, civil protection and crisis management is not streamlined and clear. Even during a cursory review of the specified sector, the incompleteness and inconsistency of the relevant legislation is noticeable.

Romania

Resilience

According to the **National Defence Strategy for 2020-2024**, consistent efforts are needed to transform our country into a **resilient state**, capable of adequately responding to the unpredictability and extent of developments in the security environment. For this, a strong state is needed, a state that is aware of the need to develop its own quick and efficient reaction mechanisms and, inherently, a solidly dimensioned security culture – including among its citizens. Flexibility, adaptability, the ability to react quickly in times of crisis are principles of strategic management, which allow anticipation and planning, and preparation for the most unfavorable cases, to avoid strategic surprise and ensure resilience and good governance for the benefit of all Romanian citizens.

The Supreme Council of National Defense (CND) is the autonomous administrative authority vested, according to the Constitution, with the unitary organization and coordination of activities related to the country's defense and national security. All institutions involved in the National Defense System are led and coordinated for the process of strengthening the state in order to become a resilient one.

At the national level, the chief of Department for Emergency Situations within the Romanian Ministry of Internal Affairs has the lead of coordinating the authorities with competences in the field of improving the resilience and implementation of the NATO's seven base line requirements.

Romania is also implementing a **Recovery and Resilience Plan within the established [Recovery Resilience Facility \(RRF\)](#)** Regulation EU 2021/241 of the European Parliament and of the Council of 12 February 2021.

[Romania's recovery and resilience plan](#) forms part of an **unprecedented coordinated EU response to the Covid-19 crisis**, to address common European challenges by embracing the green and digital transitions, to strengthen economic and social resilience and the cohesion of the Single Market.

The Plan contains 171 measures (64 reforms and 107 investments) that refer to policy areas of Euroj



Figure 1: The six pillars of the Recovery Resilience Facility⁴⁹

The coverage of the six pillars by the Romanian 15 Plan’s components is described in the table below.

Pillar I - Green transition	Pillar II – Digital transformation	Pillar IV – Social and territorial cohesion	
1 — Water management	7 — Digital transformation	10 — Local Fund	
2 — Forests and Biodiversity protection	Pillar III Smart, sustainable and inclusive growth	11 — Tourism and culture	
3 — Waste management	8 — Tax pension reforms	Pillar V - Health, and economic, social and institutional resilience	
4 — Sustainable transport	9 — Business Support, research, development and innovation	12 — Healthcare	Pillar VI – Policies for the next generation
5 — Renovation Wave Fund		13 — Social reforms	15 — Education
6 — Energy		14 — Good governance	

Figure 2: The components of six pillars⁵⁰

Legislation

The main document is the [National Defence Strategy](#), and the Law 45/1994 for National Defense of Romania published to the Official Monitor no. 172 on 07.07.1994. This law was updated with following laws, as the system adapted to the needs of the state organizational development. (They are presented in Romanian language for facile exploration of their content: Legea 58/2011 – privind modificarea art. 8 din Legea apărării naționale a României nr. 45/1994 06 mai 2011 Monitorul Oficial 303/2011, Legea 38 2002 - pentru modificarea art. 30 din Legea apărării naționale a României nr. 45/1994 31 ianuarie 2002 Monitorul Oficial 75/2002, OUG 13/2000 - pentru modificarea art. 5 din Legea apărării naționale a României nr. 45/1994 18 iulie 2001 Monitorul Oficial 111/2000, Ordonanța de Urgență nr. 21 din 15 aprilie 2004 privind Sistemul Național de Management al Situațiilor de Urgență).

⁴⁹

<https://epthinktank.eu/2022/02/02/economic-and-budgetary-outlook-for-the-european-union-2022/structure-of-the-recovery-and-resilience-facility-3/>

⁵⁰ https://ec.europa.eu/info/sites/default/files/ro_rrp_summary.pdf

Links for the documents:

1. [National Defence Strategy](#)
2. [Law no. 415 of June 27, 2002 regarding the organization and functioning of the Supreme National Defense Council](#)
3. [The functioning regulation of the Supreme Council of Defense of the Country](#)
4. [The Supreme National Defense Council](#)
5. [Law 45 1994 National Defense Law of Romania](#)
6. [EMERGENCY ORDINANCE no. 21 of April 15, 2004](#)
7. [Recovery Resilience Facility \(RRF\)](#)
8. [Romania's recovery and resilience plan](#)
9. [Commission Staff Working Document: Analysis of the recovery and resilience plan of Romania](#)
10. [Operational Arrangements between the Commission and Romania](#)

Institutions



Figure 3: Institutions involved in the national resilience system in Romania

The main institutions involved in the national resilience system in Romania are: Ministry of Internal Affairs (MoIA) Ministry of National Defense (MND), Ministry of Foreign Affairs (MoFA), Ministry of Justice (MoJ), Ministry of Economy (MoE), Ministry of Finances (MoF), Romanian Intelligence Service (RIS), Foreign Intelligence Service (FIS), Ministry of Transportation (MoT), Ministry of Agriculture (MoA), Ministry of Energy (ME). Other institutions from the national security system also contribute or support the national effort for becoming a resilient country.

The Supreme Council of National Defense (CND) analyzes and/or proposes, according to the law, the promotion of Romania's national security strategy and the country's national defense strategy, Romania's military strategy, Romania's public order and national security strategies, in relation to the responsibilities of the empowered institutions. Also, analyzes data, information and evaluations provided by the intelligence services and other structures with attributions in the field of national security in order to coordinate the measures to be taken in case of crisis, major crisis or war. The resilience of the nation relies on this structure ability to coordinate the entire national effort.

Strengthening resilience and reducing vulnerabilities calls for a flexible multidimensional strategy and a broad perspective on all systems, to reduce the risks associated with a crisis, but also to improve the ability to rapidly manage adaptation mechanisms at local, national and regional levels. Resilience covers all stages of a crisis situation, from prevention (when possible) to adaptation and mitigation (when necessary), and includes positive transformations that strengthen the ability of current and future generations to assure their basic needs. In this context, the National Defense Strategy of Romania directs the efforts subsumed under the objectives of the defense policy, in a comprehensive approach, which has in mind the strengthening of inter-institutional cooperation on all levels subsumed under national defense, including from the perspective of the resilience dimension, considering the field of responsibility of the Ministry of National Defense.^[1]



Figure 4: The process of assessing and responding to the potential risks and threats

All institutions involved in the national defense and security systems assess threats, build scenarios and propose measures and response options to CND. CND analyzes the data received, and through the prime-minister (also vice-president of CND) and the others members delivers strategic directions in order to respond properly and resiliently to potential risks and threats.

Depending on the situation, crisis management cells are created (Situational Task Force) under the prime minister's decision and the government decides which institutions should be involved.

The Ministry of Internal Affairs, through the Department for Emergency Situations - General Civil Protection Directorate, proposes the meeting of the Interinstitutional Strategic Group for Resilience. The Interinstitutional Strategic Group makes proposals to update, complete and/or modify the legal framework necessary to ensure the implementation of national resilience requirements.

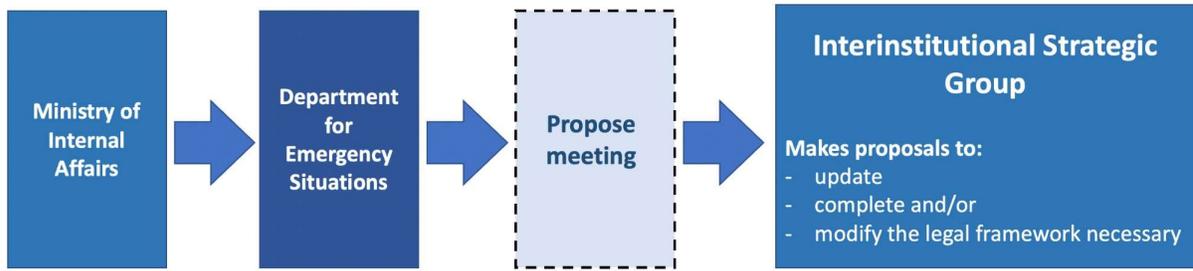


Figure 5: The process of initiation of Interinstitutional Strategic Group for Resilience

The **cooperation** between the government institutions, intelligence services and agencies is coordinated to function on vertical and horizontal communication according with the national legislation. There is a system of systems, according to different institutional competencies and the process works in a supported and supporting way.

The main crisis was the COVID-19 pandemic for which public information campaigns, viral testing and vaccination were organized. Also, there were operations for area containment, lockdowns, curfews and other measures for reducing the spread of COVID-19. The Romanian Ministry of Internal Affairs represented the lead agency, with the Ministry of Health in close cooperation and the other agencies in support.

The Euro-Atlantic Center for Resilience is an inter-institutional hub and research body that supports and participates directly in the issuing and development of concepts, doctrines, methodologies, standards and working tools in the field of resilience. The Center will carry out ongoing research in the field of resilience and strategic anticipation and will provide specialist advice and expertise in the field of resilience.

E-ARC was designed to be an important resource for the entire Euro-Atlantic area and its mission is to scan the resilience horizon as wide as possible, trying to anticipate the next major crisis, to prepare society for the unexpected, and to identify early warning signals. One of Center's main aims is to provide an intellectual framework for decision-making in the field of resilience.

The structure and working programme of E-ARC covers important fields of resilience, ensuring that the Centre is a unique and valuable institution for both NATO and the EU, capable of offering expertise in its field of responsibility. All the NATO concepts regarding resilience are considered as guidance and starting points for further E-ARC assessments and recommendations for related national entities. From this point of view, E-ARC is more related with the large area of research for resilience, while the aim of Crisis Management for Disaster Response CoE, is more specific and punctual.

At first stage, E-ARC operates as a public institution, with legal personality, under authority of the Romanian Minister of Foreign Affairs (MFA). Following the operationalization of E-ARC, its work will be internationalized by co-opting NATO and EU partners.

Conclusions

The main Resilience Strategic Document in Romania is [National Defence Strategy 2020-2024](#), which outlines assessment of the security environment; threads, risks and vulnerabilities as well as lines of actions.

Romania is also implementing a Recovery and Resilience Plan within six pillars of Recovery and Resilience Facility to address common European challenges by embracing the green and digital transitions, to strengthen economic and social resilience and the cohesion of the Single Market.

The Department for Emergency Situations within the Romanian Ministry of Internal Affairs has the lead of coordinating the authorities on the resilience and implementation of the NATO's seven baseline requirements as well as proposes the meeting of the Interinstitutional Strategic Group for Resilience.

The Euro-Atlantic Center for Resilience plays an inter-institutional hub and research body that supports and participates directly in the issuing and development of concepts, doctrines, methodologies, standards and working tools in the field of resilience.

[1] 2021 Romania's White Charter of Defence.

[2] CMDR COE is a NATO center of excellence located in Sofia, Bulgaria – with the aim of providing expertise in crisis management and disaster response

Israel

Resilience

Resilience is the ability to bounce back from a national shock and withstand serious adversity; it is the buffer capacity of a system to absorb different forms of shock. National resilience may be found in the large array of policies and resources that countries employ in order to cope with the challenges before them. This embraces the nation's readiness to contain a disaster and to maintain its social functions in an adaptive manner. National resilience refers to the measure to which the affected national community can react to a catastrophe in accordance with its severity and magnitude; and the ability of the affected community to recover from a low point of functionality to its normal or even to an improved level of functioning. National resilience in essence is the motion of a bounce-forward – the capacity of a nation to turn a crisis into a success.

Within terms of the **National Resilience System** following general pillars might be mentioned:

- National Resilience
- Organizational resilience
- Social / Community Resilience
- Personal and Family resilience / Trauma

Legislation

Civil Defense (HAGA) Law. The 1951 civil defense law, revised several times since then, legislates matters pertaining to civil defense. The law requires shelters to be built in all homes, residential and industrial buildings. The law also establishes the civil defense service, mandates the construction and upkeep of shelters in homes, residential buildings, and factories, allows the state to make use of private equipment and human power for emergency situations, defines a civil state of alert, and lays down rules regarding the use of hazardous materials.

By the Law, Knesset or the Government of Israel are to declare the State of emergency - a legal status that grants the Government authority to take certain adequate and necessary measures. Israel has formally been in a "state of emergency" since its establishment in 1948. The Knesset extends this legal status periodically.

Based on the authority granted by the Civil Defense (HAGA) Law the Minister of Defense may declare A State of Special Emergency, in a defined area in which there is a "crisis" for a limited period of time. Such a declaration temporarily transfers certain powers and responsibilities from civil authorities to the home front command and precipitates special arrangements.

Institutions

The agencies that have been granted by the Government of Israel or the Knesset **with formal responsibilities or authority** in case of a crisis. These agencies are:

- **National Emergency Authority** (Rashut Ha'Herum Ha'Leumit – **RACHEL**) in the Ministry of Defense - was created in September 2007 and charged with coordinating military and civilian action (government ministries, local authorities and public organizations) during a state of emergency, war or natural disaster;
 - **National Emergency Economy Board** (Meshek Le'shat Herum – **MELACH**), which is part of RACHEL and includes agencies in charge of the evacuation, assistance and casualties (Pinuy, Sa'ad ve Halalim – PESACH); allocation of gas, supply of electricity, water and food; provision of communication services or operation of infrastructure systems;
 - **Home Front Command (HFC)** is part of the IDF and the Ministry of Defense. The Israeli Home Front Command was created in February 1992 following the Gulf War. Ever since its creation, there have been great efforts undertaken to turn the Home Front Command into a civilian body, but thus far, all of these have failed.;
 - **The Police** - a national agency which is subordinated to the Ministry of Public Security;
 - **Fire and Rescue Services** (Mechabei Esh) - a national agency under the Ministry of the Interior;
 - **The Health Sector** - hospitals, clinics, and Magen David Adom Emergency Ambulance Service, subordinated to the Ministry of Health;
 - **The Civil Sector** - numerous local units of government including municipalities, regional, and local councils;
 - **The Environmental Sector** - the Unit for monitoring hazardous material under the Ministry of Environmental Protection.
- Civil Resilience Network** - a network composed of thousands of units (nodes) – such as

individuals, volunteers, households, businesses or organizations – that are not part of the Emergency Authorities but have a commitment to enhancing local and national resilience and core capacities to adequately respond to a crisis.

From the emergency management perspective, many Western nations struggled with the balance between an all-threats emergency management approach and a single-threat emergency management approach based exclusively on fighting terrorism. With solid emergency management planning and procedures, preparedness for one type of threat should have spinoffs and overlaps that can be applied to managing other types of threats. Israel counts on such overlaps its ability to manage all threats. Despite the presence of other threats, Israel's situation has positioned it to have a predominately single-threat approach to emergency management. Israel's emergency management system can be viewed as an example to consider where both the strengths and weaknesses of taking a predominately single-threat approach can be observed.

For a variety of reasons, the **nation-state of Israel has taken a military-centric approach to emergency management**. The structure of society, the threat environment faced, and the urgency of the dangers are some of the reasons such an approach has proven successful for Israel. Other nations have struggled with the extent to which standing military forces become involved in managing disasters. In some cases, especially with regard to warfare or terrorism, the military may be the most appropriate entity to manage the emergency. In the event of natural disasters or technological disasters, while the military may have materiel and personnel it can apply to the situation, the civilian sector may be better suited to manage the emergency. When military-based emergency management decisions are made impacting the civilian sector, questions concerning the very nature of democratic governance may not be far behind. One of the reasons driving the formation of the new National Emergency Authority in Israel is to coordinate government/military and civilian sector emergency management functions. Even with these steps towards increased coordination, one could note that RACHEL is housed in the Ministry of Defense. For comparative emergency management purposes, looking at Israel can provide a wealth of information concerning the strengths and weaknesses that a military-centric approach has towards emergency management.

Resilience practices Individual responsibility. In Israel, individuals are educated from an early age on their responsibilities during crises. The HFC educates the public about their role before and during a crisis, namely, knowing the location of their nearest shelter and seeking shelter when needed. Individual involvement in preparing for and responding to a crisis is typically mediated through the Israeli MOD and Israeli Defense Forces (IDF).

Since Israel views its citizens as not only inhabitants of its homeland but also as integrated units of the whole nation, citizen preparedness is almost a way of life for its civilians.

Education and military service

Large areas under public domain in Israel, which contribute greatly to citizen engagement leading to community preparedness, are the education system and military service. These two sectors, fulfilling the monumental roles of education and security of the nation, can be an insight into the level of trust Israelis afford their government.

Other state organisations partner with the Ministry of Education (MOE) to develop and implement these activities. The IDF, through the efforts of the HFC, provide a great deal of printed and online

materials and trainings. The Israel Police and their voluntary forces within the Civil Guard are also active participants in school trainings.

Preparedness training and exercises are components continued as mandatory training and service within the preparedness sector, and culminate in mandatory military service for most Jewish 18-year-olds.

Home Front Command and the community

The IDF is comprised of four Commands: Northern, Southern, Central, and Home Front. The IDF heavily relies upon the HFC for preparedness and response to any type of threat and civilians are a valued segment of the force structure. While the HCF is an actual component of the military, it interfaces with voluntary organisations, civilians, and professional responders to organise an integrated response to an event. Two reasons for creating the HFC were to improve coordination of government, first responders, and the military during an event, as well as provide equipment and supplies to citizens for preparedness and response. During wartime, the HCF has command and control, but during peacetime, it is in charge of national preparedness and response, and partners with the national police for readiness and emergency response. The HCF allows for greater civilian coordination, education, training, and exercising of civilians. It is also responsible for planning and deploying warning systems, may be given command and control over other response organisations during an emergency, and works with the Ministry of Health to coordinate all the primary stakeholders for preparedness.

The HFC via partnership with schools, police, fire, and voluntary organisations leads community preparedness in Israel. Beyond education and training, the HFC distributes emergency kits, gas masks, antidotes to poisonous gas, assists in logistics, evacuations, and sheltering, and provides information and guides, such as directions for building safe rooms in the home.

The public information Internet World Wide Web site for emergency management in Israel created by the HFC (Homefront Command, 2009b) lists under its "How to act in an emergency" the following hazard-related items:

- Correct behavior during missile and rocket fire
- How to behave in a rocket or mortar attack
- How to behave in an earthquake
- How to behave in a hazardous material leak
- How to behave in a flood
- First aid
- Coping with an emergency
- The national disaster drill

In addition to basic emergency practices and hazards of social origin, the public information website lists earthquakes, floods, and hazardous material leaks as other hazards of concern in Israel. It should also be noted that Israel faces potential natural hazards like earthquakes originating from the northern section of the Dead Sea Rift. In terms of technological hazards, like any other developed nation, Israel faces many technological hazards related to industry, transport, and infrastructure. The Homefront Command Search and Rescue Unit has participated in a variety of responses to technological disasters such as train crashes and building collapses in Israel and it has also assisted in foreign natural disasters. In considering Israel, the comparative strength can be drawn from observing emergency management practices in a society that takes a single-hazard approach. **Law enforcement and the civil guard**

The Ministry of Public Security supervises the Israel National Police (INP) and the Israel Fire and Rescue Services. The INP contains a volunteer unit, the Civil Guard, which was formed in 1974 following multiple terrorist attacks and is the nation's largest voluntary organization. Over 70,000 citizens participate in the nation's Civil Guard, an organization that supports multidisciplinary agencies, and is the de facto community branch of the Israeli police.

Emergency medical response, Magen David Adom, and Hatzalah

The major emergency medical service, Magen David Adom (MDA), engages volunteers to support its efforts, as do Israeli hospitals. MDA has 123 medical stations and 11 dispatch stations from which to coordinate its response. The force structure of MDA is roughly one staff person for every five volunteers, with volunteer roles in MDA mirroring those of full-time personnel. These well-trained volunteers are completely embedded members of the emergency response team.

Emergency response, religious considerations, and ZAKA

The emergency response process outlined has a duration of approximately one hour from a dispatch call until the scene is cleared and activities return to normal. This goal of swiftly returning to a state of normalcy is achieved all the while respecting religious traditions. A voluntary organization, ZAKA, is the key partner for these efforts.

RACHEL, Israel's National Emergency Authority, was established in 2007 to work with the police, fire, military, MDA, voluntary, and other local authorities in an effort to coordinate emergency response efforts. RACHEL's role is not to command and control an event, but rather to coordinate the efforts of all bodies of authority within the incident.

Following an increase in terrorist attacks in the 2000s, certain regions in Israel began to further develop a civil defence to incorporate 'resilience'. At a state and municipal level as well, civil society has started to play an important role in supporting resilience, including supporting the psychological resilience of citizens. This has led to the establishment of regional resilience centres (RCs) manned by social workers. RCs work with local councils to prepare them for emergencies, reinforce community resilience, and provide individual mental health treatments. They provide access to therapists, nurses, and social workers for the local community. Civil society, with the support of the central government together with local councils, also runs local Community Emergency and Resilience Teams (CERTs), set up and staffed by volunteers. CERTs support communities during emergencies and provide medical, psychological, and social assistance to the local community.

Government structures Israel established a National Emergency Authority (NEMA) in 2007, following the Second Lebanon War. NEMA aims to improve interagency cooperation and to emphasise a non-military response to emergency management. It plans for emergency situations and coordinates with national and local authorities in order to maintain national resilience. In addition to NEMA, several other government agencies contribute to resilience in Israel. The Ministry of Economy's Emergency Food Supply Division advises civilians about appropriate individual stockpiling and does contingency planning, including recommendations for stockpiling certain key food items. The Ministry of Health also has an Emergency Department that stockpiles imported medical products in case of an emergency.

The HFC is (1) providing citizens with shelter when the country is under attack, and (2) planning and preparing so that citizens know in advance what to do in an emergency. The HFC works closely with the IDF, ensuring that communication and operations networks between the civilian and military sides are well-maintained, such that they can easily be activated in the case of a crisis. The HFC

also operates early warning sirens that all citizens receive on their mobile phones, warning them to go to a shelter.

Besides others, the issue of **Social / Community resilience** seems to be very interesting and even unique by approach. Resilience is a significant factor in coping with the psychosocial consequences of disasters and terrorism. The focus on resilience-building in emergency management is well established in Israel. Nine Community Resilience Centers have been operating in Israel since 2007. Each is made up of the following interdisciplinary teams: a security committee, a community development team to provide physical/psychological support, a psycho-trauma treatment team to treat special needs groups, absorption, community information and communication, an economic/social team, a fundraising team, an education team, a culture and leisure team, and a training committee. Five of these centers have already been tested in real crisis situations and were very effective in coordinating and managing the psychosocial needs of the communities through deploying trained community workers, activating hundreds of volunteers, operating the psycho-trauma center, coordinating the involvement of NGOs and other donations from the outside, operating helplines and information centers, running alternative education and schooling activities in shelters, and providing basic needs to vulnerable populations.

The emergency behavioral management system. In recognition of the critical role of behavioral response in all phases of emergency management and the importance of mitigating the psychosocial consequences of disasters and mass violence, we suggest that an emergency behavioral management system (EBMS), focusing on the psychosocial aspects of disasters and including defined roles for emergency behavioral officers (EBOs), be further developed and integrated into the current models of emergency management now in place

The task of the EBMS include (a) advising policymakers, (b) building databases, (c) developing tools and methods to analyze information in “real-time,” and (d) coordinating agencies and services dealing with the public during normal times so that the response during the emergency will be well organized and resources will be better used. With terrorist attacks, it must take into account additional considerations, including the public’s reaction to the perpetrators (such as the wish for revenge, which is not always directed at only the perpetrators) and the altered perception of what constitutes a safe activity (such as fears of traveling on a bus and eating in a café). The EBMS should function at all levels: (a) headquarters (decision makers), (b) intervention teams, and (c) ground level (in the community). At the local level, it should adopt the concept of “helping the public to help themselves”; that is, enhancing “motivational resiliency” and the concept of “assisted coping” (i.e., doing with rather than doing for people to foster a sense of self-efficacy).

Conclusion

The Israeli resilience being heavily sponsored by the armed forces has successfully met the challenges of terrorism, rockets, and missiles, which have replaced the conventional threat as Israel’s principal challenge. Yet in addition, Israel must exhibit social and cognitive resilience, which encompasses several internal factors that threaten to undermine this stamina: efforts at democratic economy legitimization, economic gaps, the debate on the Palestinian conflict, and the reduced adulation of law enforcement, and the challenge to the courts. The answer to these challenges,

particularly in the absence of an existential security threat, is the redirection of resources to the internal arena to correct what must be corrected.

The last war in which Israel was called on to use all of its force was the Yom Kippur War (1973). Since then, Israel had been challenged by clashes, conflicts, and wars that did not require taping all of its power. Instead, the main element put to the test was the endurance of Israeli society.

Israel has always faced significant challenges to national security and thus has had certain resilience-enhancing measures in place for decades. These measures have not always been implemented with the stated aim of increasing resilience, but can be classified as resilience-enhancing, namely that these measures allow 'the capacity to prepare for, to respond to, or to bounce back from problems or perturbations'. The frequency of conflicts in Israel's history, including a series of wars, Palestinian uprisings, armed conflicts, and terrorist attacks, has led to Israel's emergency management being highly military-centric. However, it should be noted that Israel is by no means immune to natural and technological threats. It would be remiss to say that other threats play no role in Israel's emergency management. The capabilities of the Israeli crisis management system to withstand threats and challenges were, in particular, thoroughly and vividly demonstrated during the COVID-19 pandemic.

Ukraine and Israel have notable differences including land mass, population, nature of threats; cultural and religious homogeneity; as well as levels of public trust in government. However, the contextual differences are not leading to prevention for utilizing best practices from Israeli community preparedness models and applying them to Ukraine. Many Israeli practices parallel those of Ukraine, particularly the utilization of volunteers in disaster preparedness and response. Israel's history of threats and the resultant citizen engagement model have made Israel the leader in utilising civilians as a force structure component for community preparedness and national resilience. Since portions of Israel's model have demonstrated success, and are applicable, these practices should be implemented to increase Ukraine's community preparedness and resilience.

United Kingdom

Resilience

Resilience has traditionally been a fundamental part of the UK's approach to national security. The 2021 Integrated Review of Security Defence, Development and Foreign Policy¹ recognised that in an increasingly interconnected and unpredictable world the UK needed to enhance and broaden resilience as a national endeavour, so that the UK is better prepared for future crises.

COVID-19 was a sharp reminder to the UK that security threats and tests of national resilience can take many forms. The UK's approach to developing national resilience starts at home, defending the people. The UK's territory, critical national infrastructure, democratic institutions and way of life. It is designed to protect wider and softer aspects of national security. Globally, the world is becoming more interconnected and contested; an incident such as COVID-19 rapidly has global and systemic consequences that are not easy to predict, mitigate or recover from. UK's resilience is therefore interconnected to global resilience and requires improvement.

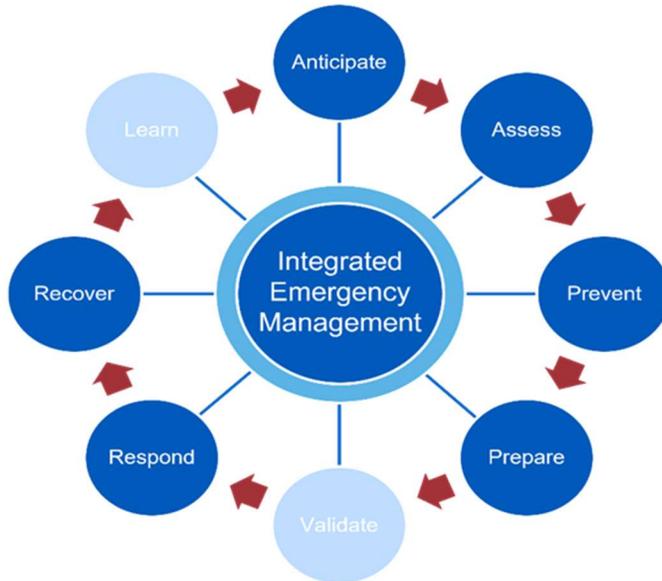
The UK is committed to enhancing its national resilience and that of the Alliance. The UK approach is consistent with the 2016 Warsaw Summit commitment to achieving 7 baseline requirements for civil preparedness, reflecting that the resilience of civil structures, resources and services is the first line of defence. The development of the UK's national resilience system is not directly attributed to NATO, though many of the key principles espoused by NATO are embedded in UK systems and approaches.

Legislation

The UK is seeking to learn lessons from its response to COVID-19 through the development of a National Resilience Strategy that is designed to improve national preparedness and readiness from early warning to recovery. This is being taken forward in an integrated way to include actors at national strategic and local government levels, but also includes business and civil society. A number of actions have been defined for this work:

- Establishing a ‘whole-of-society’ approach to resilience. This will include improving government communications to the public on preparedness; developing sector-specific legislation and embracing UK’s resilience to cyber risks
- Assessing threats and hazards to build national resilience across the broad range of risks facing the UK, from malicious and non-malicious, direct and indirect, and acute and chronic – including low-probability, This will mean integrating national security with economic, health and environmental policy spanning the breadth of risk from anticipation, prevention, preparation, response and recovery.
- Linking domestic and international actions and placing more emphasis on tackling, even disrupting, risks at source.
- Developing more capabilities, including people, skills, technology and equipment to enhance resilience. This includes testing capabilities through contingency planning and regular exercises, bringing together all instruments from across government, the emergency services, the armed forces, other local responders and industry
- Reviewing UK’s approach to risk assessment (risks are contained in a classified National Security Risk Assessment that lists and assesses the impact and likelihood of the most serious risks facing the UK and its interests overseas).
- Strengthening UK’s analytical, policy and operational tools – including the collection and use of data. This will include establishing a new Situation Center. This will provide data and analysis, and encourage collaboration across government to inform crisis decision-making. Security and intelligence agencies will better synthesize intelligence and open source information using cutting edge digital technology.

The UK’s approach to resilience is founded on the following phases defined in emergency management.



· **Anticipate:** Involves organizations individually and collectively, horizon scanning for emerging and changing risks. These risks may appear outside of the UK.

- **Assess:** Assessing risks, setting priorities and determining likelihood of the risk occurring.
- **Prevent:** The best way to manage risk is to prevent it impacting in the first place.
- **Prepare:** Planning, training and exercising
- **Respond:** If preparation (above) is undertaken efficiently then the response is likely to be effective.
- **Recover:** This is about recovering to the 'new normal'.
- **Validate** and **Learn** are important elements providing opportunities to refine and improve the process through assessment and analysis.

The Civil Contingencies Act 2004[1] provides the legislative framework for the UK's planning and response to various types of emergencies. The Act is divided into three parts: Part 1 defines the obligations of certain organizations to prepare for various types of emergencies; Part 2 provides additional powers for the government to use in the event of a large-scale emergency; Part 3 provides supplementary legislation in support of the first two parts.

[1] <https://www.legislation.gov.uk/ukpga/2004/36/contents>

Institutions

The UK has a dedicated Minister for Resilience. The Civil Contingencies Secretariat (CCS) in the Cabinet Office coordinates the UK's resilience to the full range of emergencies. Central government, through the Cabinet Office, works very closely with the devolved administrations, local authorities and emergency services. The CCS works closely with a wide range of other stakeholders. Within the CCS, is a Planning and Analysis Secretariat that is responsible for longer term work to enhance resilience, as well as providing data and analytical support to decision making. A National Resilience Framework Team leads on taking forward work on national resilience, managing the resilience system and risk processes.

The CCS supports the Civil Contingencies Committee (CCC), also known as COBRA. The CCC is the forum for ministers and senior officials to manage serious and catastrophic emergencies, domestic and international, malicious and non-malicious. The composition of this committee depends on the nature of the incident but it is usually chaired by a minister, sometimes the Prime Minister. Other key ministers, mayors, police chiefs and national and local government representatives will be present. The UK has adopted the concept of Lead Government Department[1], where lead responsibilities for planning, responding and recovering from emergencies are allocated to Ministries/departments, dependent on the nature of the emergency.

A multi-agency/integrated and vertical approach provides the framework for the UK national resilience system. Under these arrangements a framework is established to ensure integration between national and regional and local actors⁵¹.



At the regional and local levels Resilience Forums are established; multi-agency participants that convene for emergency preparedness, anticipate, assess, prevent, prepare etc and can provide a local strategic coordination function⁵².

In assessing threats, building scenarios and delivering proper responses Ministerial direction is provided through the CCC and overseen by the CCS. At the local/regional levels this is undertaken through the National Resilience Forums. Key agencies, such as local authorities, police forces, fire services, ambulance services, coastguard health services, Health Protection Agency, port authorities, Environment Agency, will do a lot of this themselves in their sector specific areas of responsibility.

Conclusions

UK is experiencing a highly developed system of resilience being a long time part of national security and therefore committed to strengthening both its national security as well as those of the Alliance. Terrorism, COVID-19 pandemic, climate change, organized crime fostered UK since 2014 to build-up its resilience and prepared new National Resilience Strategy (autumn 2022). It is designed to improve national preparedness and readiness from early warning to recovery and is based on the 'whole-of-society' approach to resilience. This will include improving government communications to the public on preparedness; developing sector-specific legislation and embracing UK's resilience to cyber risks.

General Conclusions

The importance of the topic of national resilience is recognized by all states and international organizations. The social importance and significance of national resilience is constantly growing. However, we do not currently see clear, “universal” approaches either at the national level or at the level of international security organizations. In such conditions, countries try to create their own national models, while the depth and degree of detailing of these models are very variable and often depend on the historical or current experience of the need for practical application (activation) of national resilience systems.

Traditionally, resilience is being viewed as a part of the national security system approach. In this regard, according to decisions taken by Allies on the basis of consensus, resilience of Allied Nations is also a collective commitment. NATO member states are enhancing their own resilience, including through nationally-developed goals and implementation plans, guided by objectives developed by Allies together.

Countries that were observed in this document have some differences in their approaches to resilience. Thus, it can be seen in three dimensions: 1. Countries - NATO and EU Members have a tendency to balance the development of national resilience capabilities with military, financial and other support from EU or NATO (e.g. Baltic countries, Finland, Poland, UK, Romania, Bulgaria); 2. Countries that are not NATO Members mostly rely on their own national capabilities that are strengthened by partners beyond any blocs and alliances (e.g. Israel); 3. The nuclear-weapon States, irrespective of their membership (e.g. UK), combine national capabilities, partnership support and nuclear deterrence as a strong and decisive factor.

Resilience has become a new compass for EU policies with the COVID-19 crisis. It is the ability not only to withstand and to cope with challenges, but also to undergo transitions in a sustainable, fair, and democratic manner. The crisis has underscored the importance of future-proofing EU policies and of refocusing them around resilience.

The EU's resilience is presented in four interrelated dimensions: social and economic, geopolitical, green and digital. The resilience dashboards were presented aiming to capture social, economic, and health aspects related to COVID-19, using a first selection of easily available and ready-made indicators from publicly available data sources.

On the other hand, Israel relies more on the partnership approach with EU and NATO prioritizing its national capabilities as well as cooperation with the US.

The COVID-19 outbreak became a lesson learnt to review countries national security strategy or even develop national resilience strategies (UK) in order to make national preparedness more efficient.

The comprehensive security model in Finland encompasses various levels and actors of society. Together with the central government, the authorities, business operators, regions and municipalities, such actors as universities, research institutions, organizations, other bodies and individuals form a network of comprehensive security in which the sharing of information, setting of joint objectives and commitments to cooperation can take place in a flexible manner.

Baltic states crisis management system is centralized, i.e. it represents a strict top-down structure controlled by the central national civil protection authority supported at the local level by the civil protection entities coordinating civil protection measures in crisis situations in the administrative territories. The resilience capability of Baltic states to prevent and avert security threats depends on

the readiness to maintain critical services. The prevention of social risks is addressed in the national economic and social policy. Constant risk evaluation and monitoring is conducted in order to prevent interruption of services as well as update the CM action plans. In particular, Estonian focus on e-services could be essential to develop more digital solutions within the cyber domain.

The case of Romania demonstrates to us that long-term strategy orientation in the domain of resilience is proven to be sustainable and efficient. Moreover, its national resilience system also integrates eco-challenges. The Ministry of Internal Affairs is the leading body in terms of coordinating national efforts in resilience and implementation of NATO baseline requirements.

The concept of resilience within a Bulgarian security context is still being debated by the society. In particular, Bulgaria is continuing to research for its the most efficient option on how to link resilience to other national security concepts better.

Poland is taking only the first steps to integrate the concept of resilience into governance practice. But the high institutional capacity of state bodies and the support of various social groups allows the government to successfully implement effective solutions that actually strengthen the resilience of the state and society. Constancy and consistency of the foreign and military-political course for joining NATO and the EU in a dynamic security environment is another key factor that contributed to the achievement of positive results in the governance practice of Poland regarding the management of the development of the national security system. To strengthen national resilience Poland relies on a harmonious combination of its own capabilities and expanding cooperation within the EU and NATO, as well as on a strategic partnership with the United States.

Historically Israeli model of national resilience is heavily sponsored by and depends on military structures which have strong influence and wide authority. Israeli society is convinced that they have sufficiently stable democratic institutions and do not see the transfer of such broad powers to the military as a threat to democracy. In Ukraine, the situation may be somewhat different, and there is certain skepticism that society and politicians are ready to give the military such broad powers even during crisis situations. Therefore, the Israeli model of distribution of powers and responsibilities in the field of ensuring national stability is unlikely to be fully applied in Ukraine.

Recommendations

1. Due to the aggression of the Russian Federation against Ukraine, the key task of the state and society is to defend its independence and build a state system capable of protecting itself and its citizens. The National Security Strategy of Ukraine is based on such principles as deterrence, resilience, and liaison. Moreover, the Strategy defines the deterrence and liaison principles as Ukraine's capability development principles, including in defence and security, strategic relations with key foreign partners, etc. At the same time, resilience should imply the ability of society and the state to promptly adapt to security environment change and function sustainably, in particular by minimizing external and internal vulnerabilities.
2. It must be stated that Ukraine in its work to create a system of national resilience can only take into account some elements that exist in other countries, as well as recommendations on general goals and approaches provided by international organizations, and the practical construction of the national system will have to be planned and carried out independently. However, bearing in mind Ukraine's aspirations for NATO membership, it is highly recommended to fully align its implementation plan to meet NATO's seven baseline requirements and later amplifications.
3. To strengthen the resilience implementation process, Ukraine might consider bilateral cooperation with the few countries that are at a nearly similar level of expertise and knowledge as Ukraine.
 - a. Work with **the UK** to develop a detailed implementation plan and establishment of an overarching structure to both ensure the required cross-sectorial cooperation and coordination, as well as the capability to identify national vulnerabilities and detect, deter, and respond to hybrid threats.
 - b. Work with **Finland** to gain insight into the basis for the functioning of its national structure which is linking and coordinating the collective efforts of the central government, ministries, agencies and other public authorities, regions and municipalities, businesses, universities, research institutions, and other organizations involved in the network of comprehensive security.
 - c. Work with **Poland** to further strengthen the strategic partnership with a country with a common perception of risks and threats, shared history and culture, and despite its present shortcomings within the field of resilience, high prioritization on the implementation of a national system of resilience.
4. It is recommended to develop a Ukrainian Resilience Strategy and view it as a long-term document. The document has to be prepared based on assessment of the current security situation and identifying priority elements / issues to be addressed. Similar to Finnish and Romanian strategies, it is recommended defining in the Ukrainian Resilience Strategy a list of main institutions and actors involved as well as their responsibilities. Threat and risk scenarios and the national risk assessment has to be prepared in a way defined in Finnish Security Strategy.

5. It would be useful for the State Commission on Technological and Environmental Safety and Emergency Situations to closely look into some elements of Lithuania's crisis management system. Hence, such an institution could benefit to have practical lessons learnt as fast as it is responsible for organizing emergency prevention and direct emergency relief actions on the national level; and at local level - the Local Emergency Commission.
6. It is also worth recommending the example of Lithuanian Emergency Management Centre to be established in Ukraine to function as a permanent institution of the Emergency Commission having the function of a Government institution. In the event of emergencies the Emergency Management Centre has to adopt and submit to the ministries, other public administration institutions, local authorities and the population mandatory decisions on localisation and mitigation of the effects of an emergency.
7. As organic part of the Emergency Management Center it is recommended to establish a Center of Excellence on national resilience as inter-institutional hub and research body that supports and participates directly in the issuing and development of concepts, doctrines, methodologies, standards, working tools, study programs in the field of resilience, conduct related studies, collect and share experience, deliver specific trainings to the specialists working in the area of national resilience.
8. It is vital to start the process of collecting Lessons Identified within all sectors of society. It is crucial to identify both strengths and weaknesses in the existing system to develop a robust implementation plan. This requires a transparent and inclusive process that avoids attributing responsibility and blame for failures identified.
9. It is recommended to establish an overarching structure to both oversee the capturing of Lessons Identified and the ensuing analysis, develop a strategy and guidance for the implementation of the concept, ensure a link to ongoing reform processes, and build a structure capable of detecting, deterring, and responding to hybrid threats. This includes the ability to:
 - a. Establish and maintain cross-sectorial situational awareness.
 - b. Detect trends, outline response options, and deliver strategic cross-sectorial advice on how to respond jointly.
 - c. Identify vulnerabilities open for exploitation and develop threat scenarios based on synchronised employment of both military and non-military means.
 - d. Make regular cross-sectorial risk assessments. Design and implement policy to minimise risks.
 - e. Closely coordinate Ukrainian cross-sectorial response, using Ukraine's total resources.
10. A new approach to engaging citizens in preparedness and resilience in Ukraine is needed to increase community preparedness. Examination of Israel's proven model of community preparedness has shown that applying, adapting, and utilising some of these components will greatly enhance Ukraine's resilience. The government's role is to design and resource flexible programs communities can tailor to address specific threats, needs, and strengths unique to their citizens and society.

Appendix

Annex 1. Questionnaire for Experts

QUESTIONNAIRE

On the Experience of individual states to form and institutionalize the national resilience system/crisis management system

1. Could you please provide a brief description of the national resilience system of your country? What legislative acts regulate the functioning of the national resilience system? Could you provide links to the laws?
2. What institutions or organizations make up the national resilience system in your country? Could you, please, briefly describe the hierarchy, functions, responsibilities?
3. Who assesses threats, builds scenarios, develops response options, and delivers strategic cross-sectoral direction on how to respond to potential risks and trends?
4. Could you present the scheme of interaction between various institutions of the national system of resilience? How interagency coordination is carried out within the framework of the national resilience system?
5. What was the major threat for your country since 2014 and what key prevention/mitigation measures were addressed?
6. What role do the NATO Resilience Committee and the Center of Excellence for Resilience (CMDR CoE) play (if any) in building your country's national resilience system.

Annex 2. Logic Model

G O A L	Effective interaction of the state and society to systematically prevent, conduct proper response and rapid recovery after crisis situations			
	<p>1. Identification, assessment and prioritization of risks and threats is carried out in a systematic and coordinated manner</p>	<p>2. Decisions to prevent and respond to risks are made and implemented systematically on the basis of complete information</p>	<p>3. Overcoming the consequences and post-crisis recovery is based on the systemic interaction of state and non-state actors</p>	<p>4. State institutions have sufficient capacity to monitor the implementation and evaluate the effectiveness of the adopted decisions to prevent and respond to risks</p>
	<p>1.1. To form a coordination mechanism of state bodies and non-state institutions regarding the identification, assessment and prioritization of risks and threats, the effectiveness of its application</p>	<p>2.1. To form a mechanism of coordination, exchange of information and situational awareness of state bodies and non-state institutions to prevent and respond to risks</p>	<p>3.1. To form a mechanism of coordination, exchange of information and situational awareness of state bodies and non-state institutions in the event of a crisis situation</p>	<p>4.1. To form the institutional capacity in state bodies for monitoring and evaluating decisions and measures to prevent and respond to risks</p>
	<p>1.2. Carry out an analysis of the current regulatory and legal basis for the identification, assessment and prioritization of risks and threats, the effectiveness of its application</p>	<p>2.2. To form a decision-making mechanism (government institution) to prevent and respond to risks</p>	<p>3.2. To develop a procedure for forming a decision-making mechanism (government institution) in case of a crisis situation</p>	<p>4.2. To develop a methodology for monitoring and evaluating decisions and measures to prevent and respond to risks</p>
<p>1.3. Study and adaptation of best international practices regarding identification, assessment and prioritization of risks and threats</p>	<p>2.3. To develop ongoing instructions and protocols for preventing and responding to risks</p>	<p>3.3. To provide appropriate capabilities, substantiation and formation of necessary reserves in case of crisis situations</p>	<p>4.3. To develop a procedure for monitoring and evaluating decisions and measures to prevent and respond to risks</p>	
T A S K S				

<p>1.4. To develop united approaches (principles, processes and mechanisms) for identification, assessment and prioritization of risks and threats compatible with NATO practice</p>	<p>2.4. To implement united instructions and protocols for risk prevention and response for all government agencies</p>	<p>3.4. To provide a mechanism/procedure for restoration of reserve capacities of critical infrastructure objects</p>	<p>4.4. To provide resources for monitoring and evaluation on a regular basis</p>
<p>1.5. Implement united approaches for the identification, assessment and prioritization of risks and threats for all government bodies</p>	<p>2.5. To establish a Center of Excellence (for studying, summarizing and disseminating the best domestic and international practices)</p>	<p>3.5. To develop methodologies for assessing damage caused by crisis situations</p>	<p>4.5. To establish a system of training and raising the level of professional competence of civil servants in matters of monitoring and evaluation</p>
<p>1.6. To elaborate a training system for the identification, assessment and prioritization of risks and threats, the effectiveness of its application</p>	<p>2.6. To develop a system of training civil servants on crisis management issues and promote the creation of appropriate training programs for representatives of the non-state sector</p>	<p>3.6. To develop procedures for assessing the resources necessary for eliminating the consequences of crisis situations and post-crisis recovery, determining sources and procedures for attracting resources</p>	<p>4.6.</p>

Annex 3. Extra Sources

1. [A Route to National Resilience. Building Whole-of-Society Security in Ukraine \(en\)](#), Report of the [International Centre for Defence and Security](#) (Tallinn, Estonia).
2. [“Building national resilience. Aligning mindsets, capabilities, and investment”](#), Publication of the Marsh & McLennan Companies
3. [“Forward Resilience: Protecting Society in an Interconnected World”](#), Publication of the [Center for Transatlantic Relations](#) (Washington, DC). In particular, see Executive Summary, Chapter 5 “Resilience Inside and Out: A Finnish Viewpoint” and Chapter 7 “The Case for Forward Resilience in the Baltic States”.
4. [“NATIONAL RESILIENCE INDEX 2020: AN ASSESSMENT OF THE D-10”](#), Publication of The Henry Jackson Society (London, UK)
5. Extra national specific cases:
 - Japan [“Fundamental Plan for National Resilience - For Building a Strong and Flexible Country”](#) and [“Building National Resilience”](#)
 - Australia [“A National Resilience Framework for Australia”](#)
 - Malawi [National Resilience Strategy \(2018 – 2030\)](#)
 - The Commonwealth of Dominica [National Resilience Development Strategy 2030](#)

Annex 4. Focus Group Experts

1. **Adrian Duta**, Vice President, E-ARC, Romania
2. **Phil Jones**, PROTECT international advisor
3. **Hans Petter Midttun**, PROTECT international advisor
4. **Plamen Pantev**, Director, Institute for Security and International Studies (ISIS), Bulgaria
5. **Vitalijs Rakstins**, Head, Crisis Management Department in Ministry of Defence of Latvia
6. **Valeri Ratchev**, expert, Center for Security and Defence Management at the Bulgarian Academy of Sciences



Alinea is an international development consultancy providing technical and management expertise that helps people improve their lives. We work with governments, investors, companies and communities to create lasting change. Over 35 years, Alinea has successfully delivered more than 515 projects worldwide. alineainternational.com