Chapter 3
WORLD EXPERIENCE OF ENSURING RESILIENCE IN THE SECURITY SPHERE

The matter of national resilience has become of major importance for most of the European countries, as well as has acquired a new meaning for the international organizations with of new challenges and threats including hybrid ones, especially after 2014. The unexpected varied manifestations of such threats have had an impact on the international security and demonstrated a weakness of a number of political instruments and institutions (first of all, UN and OSCE) that had been providing peace and stability after World War II. Even more attention has been attracted to the issue of national resilience under conditions of the COVID-19 pandemic.

Significant changes in the global security environment have encouraged both individual states and international organizations to revise their conceptual approaches to ensuring state and society resilience in order to adapt them to new conditions. The world's leading countries and international organizations now deem that the objectives of developing and implementing new national resilience ensuring mechanisms and improving the existing ones are now of a high priority.

At the same time, in the last years, various states` and international organizations` practices and some experts` recommendations containing the term “resilience” in their contents have become more popular. This raises the need to examine them for correspondence with existential features of the interdisciplinary concept of resilience in the national security sphere.

1

3.1. NATO Goals and Objectives with regard to Building National Resilience

3.1.1. NATO's Response to Changes in Global Security Environment after 2014

The main goal of NATO`s establishment in 1949 was to unite efforts to form a collective defense and safeguard peace and security. In particular, Article 3 of the North Atlantic Treaty (NATO, 1949) reads that in order to achieve more effectively 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 5 of this document specifies the principle of collective defense defining an armed attack against one or more Member States as an armed attack against them all. Thus, North Atlantic Treaty founded the resilience potential of this organization and of Member States thereof if we view it through a prism of military cooperation, deterrence, and readiness to repeal an armed aggression. Here, major importance belongs to the issues of interoperability of armed forces, creation of conditions for their effective deployment and support on the territories of Alliance Member States.

When the hybrid aggression of Russian Federation against Ukraine started in 2014, it became clear that the stated principles are surely necessary but still insufficient to effectively counter the new threats and challenges. As Lasconjarias (2017) noted, the initial NATO's reaction to Russia`s aggression against Ukraine in 2014 was highly political and very conventional.

General Breedlove (2015), Commander-in-Chief of NATO forces in Europe, insists that in order to respond properly to hybrid threats, it is necessary to quickly recognize and attribute hybrid actions and anticipate both conventional and unconventional activities. Such proactive steps require cooperation at all levels, from various ministries and various spheres

(diplomatic, political, informational, economic, financial, intelligence, human rights, etc.) through the implementation of the comprehensive approach. Breedlove (2015) concludes that the efforts at national, bilateral, and collective levels within NATO need to be integrated and strengthened. In addition, it is necessary to develop resilience and preparedness to resist hybrid actions including the ability for quick decision-making.

NATO Wales Summit declaration (NATO, 2014) approving NATO Readiness Action Plan was to suggest a response to significant changes that had taken place in the international security environment. Sill, having analyzed this Plan, one can conclude that the main actions proposed in the document mostly foresaw an increase in military presence, augmentation of capabilities, and intensity to ensure the collective defense, security, and deterrence on the Alliance's Eastern flank. In other words, it was about strengthening the force component of the collective defense. At the same time, less attention was paid to the enhancement of the Alliance's adaptability to new security conditions through the development of systemic links and expansion of cooperation. Thus, NATO Wales Declaration identified only a general outline and prospective changes in NATO with respect to the development of solutions allowing for a more efficient response to a wide spectrum of crises including the development of strategic communications, counteracting hybrid threats, enhancement of crisis management, planning and exercising collective defense activities, etc.

In view of the durable nature of hybrid threats and the increase of the resilience significance for NATO and the Member States, the NATO Summit in Warsaw (8-9 July 2016) approved a number of documents on additional measures to strengthen collective defense, to enhance crisis management, to develop security cooperation and also to outline new directions of activities aimed at ensuring resilience in the context of Alliance's long-term adaptation to new security conditions.

In particular, during this Summit, the Heads of States and Governments agreed on Commitment to enhance resilience (NATO, 2016b), which defines resilience as an essential basis for credible deterrence, defense and effective fulfillment of the Alliance's core tasks. This document stipulates that now the states are facing a wider spectrum of military and non-military challenges and threats including hybrid ones, which is expanding at a great pace. Under such circumstances, the protection of the population and territories requires not only adequate capabilities and armed forces' readiness to respond to threats but also the civil preparedness including continuity of governance and essential services, security of critical infrastructure, sustainable development of state and society, etc. As a consequence of large-scale and multifaceted aggressive actions of Russia at the international arena, NATO seeks to enhance the resilience of the Member States in both military and civilian areas viewing the resilience as one of the major factors ensuring effectiveness and combat efficiency of the NATO defense system. The aforementioned Commitment to enhance resilience identifies seven baseline requirements to strengthen the resilience of the Alliance and its Member States, which will be described in detail later.

According to Kramer, Binnendijk and Hamilton (2015), in presence of hybrid threats, approaches to defense support need to be expanded. Traditional measures of territorial defense and deterrence need to be complemented with modern approaches to resilience, which requires the development of capabilities that would allow for anticipating, preventing, and responding to threats that can cause destructive consequences, first of all to the key functions. The researchers note that if NATO continues limiting its role exclusively to military operations without paying any attention to the protection of its own population, the support of the Alliance will decrease. Hence, measures to counter the hybrid war need also to include new civilian-military interaction mechanisms (Kramer, Binnendijk and Hamilton, 2015).

The aforementioned issue has become now especially relevant for NATO also because a certain part of the needs of the armed forces of most of the Member States are covered by private companies. The same applies to providing a number of critical services to the public. According to NATO (2021d), almost 90% of the military transportations in support of major military operations are freighted or requested through the private sector; more than 30% of satellite communications used for defense purposes are supported by the private sector; about 75% of host nation support to NATO operations are ensured by the local businesses.

Hence, for NATO, the matter of resilience is one of the priorities because the Member States' ability to ensure proper governance, security of public institutions, and guaranteed critical services will allow for not only protecting the public but also for guaranteeing civilian support to military operations.

Lasconjarias (2017) stresses that an important NATO's objective is to strengthen civil preparedness. According to the researcher, this is stipulated not only by the need to ensure public support but also by the requirement to comply with the basic values pinpointing the Alliance's foundation, first of all, with respect to the governments' care about their citizens. Also, Lasconjarias (2017) mentions that during the Cold War and till the late 80's - ties of the past century, NATO had policies and planning called "Civil Preparedness and Civil Emergency Planning" while NATO structures included eight civil wartime agencies, covering shipping, inland surface transport, aviation, insurance, supplies, oil, and refugee movements. After the end of the Cold War it was believed that the risks of a full-scale armed aggression was reduced, so the cost of maintaining ramified civil protection systems became too high. Then, NATO, the EU and the Member States restrained their respective programs.

According to NATO (2001), Alliance's Civil Protection Committee was established in 1951, the disaster assistance mechanism was agreed upon in

1963 and NATO disaster support procedures to the Member States were approved in 1958 and remained effective until 1995 when a new mechanism for the Partner States was approved. In December 1997, to support and complement the respective UN system, it was decided to establish the Euro-Atlantic disaster response system.

In 1998, the Euro-Atlantic Disaster Response Coordination Centre (EADRCC)[1] operating 24/7 as an information system to coordinate assistance requests and suggestions, mostly in case of natural and man-made disasters, was established. The Centre also plays an important role in emergency planning. In addition, the disaster response mechanism foresees engagement of a multi-national civilian and military force group in case of a major natural or man-made disaster in a NATO Member or Partner State.

Nowadays, Alliance is consolidating its effort in this area, and matters of civil protection in the Member State are coordinated within NATO's Civil Emergency Planning Committee, CEPC[2] .

Roepke and Thankey (2019) emphasize that resilience enhancement through civilian preparedness is of major importance for strengthening deterrence and defense capabilities of the Alliance. The researchers note that the states where the governments, as well as the public and private sectors, are involved in civil preparedness planning are more resilient, have fewer vulnerabilities that can be used by an enemy as influence leverages or targets. Hence, an important aspect is deterrence by denial because it implies dissuading an enemy from aggression through persuasive proof that such an attack will not achieve the intended goals Roepke and Thankey (2019).

At the same time, Hartmann (2017) notes that until recently, the Alliance used to focus more on technical aspects of resilience as a means to ensure prompt military operations rather than on implementation of a conceptual

[1] *Euro-Atlantic Disaster Response Coordination Centre*. https://www.nato.int/cps/en/natohq/topics_52057.htm
[2] *Civil Emergency Planning Committee*. https://www.nato.int/cps/en/natohq/topics_50093.htm

principle of resilience at the strategic level. According to this researcher, under hybrid aggression, the effectiveness of the use of conventional armed forces, even to conduct large-scale operations within the collective defense, will remain limited, unless the processes of the strategy formulation are not essentially improved. It should be noted in this context that under the modern conditions, protection of the information in cyber-space becomes especially relevant. Sky-rocketing development of information technologies implies that NATO search for new ways to defend against cyber-attacks including attacks against military and civilian informational infrastructure and for the ways to enhance resilience of the Alliance and the Member States.

In order to share experiences that are useful to develop NATO doctrines and program documents and to enhance Member Nations' interaction including the area of response to new challenges, NATO Centers of Excellence have been established and are operational[3]. They are international military organizations engaged in teaching and training leaders and specialists from NATO Member and Partner States, thus performing an important mission of sharing knowledge concerning existing and potential threats and challenges. Conclusions and experiences resulting from the aforementioned Centers' efforts contribute to further transformation of the Alliance.

Operational areas of the Centers of Excellence meet NATO needs in both enhancing interaction in the military sector and sectors of crisis management, civil protection, etc. As of now, there are 27 NATO-accredited Centers of Excellence which include: Civil-Military Cooperation Center in the Hague (Netherlands), Cooperative Cyber Defence Center in Tallinn (Estonia), Counter Intelligence Center in Krakow (Poland), Crisis Management and Disaster Response Center in Sofia (Bulgaria), Center of Defense against Terrorism in Ankara (Turkey), Energy Security Center in Vilnius (Lithuania),

[3] *NATO Centres of Excellence*. https://www.nato.int/cps/en/natohq/topics_68372.htm

Center for Military Medicine in Budapest (Hungary), Modeling and Simulation Center in Rome (Italy), Strategic Communications Center in Riga (Latvia) and others. NATO Brussels Summit Communique of 14 June 2021 informs on the establishment of new NATO Centers of Excellence, in particular, Center for Resilience in Romania and Space Center in France (NATO, 2021a).

As it was noted by Tarry (2021), who was Director of NATO Defense Policy and Capabilities, resilience has always been a central idea of providing peace and security. In a complicated and unpredictable security environment it is extremely important to be prepared for threats and challenges yet before they arise. This expert believes that it is achievable through the "whole-of-society" approach. Tarry (2021) also stressed that for NATO the resilience means, first of all, availability of resources, infrastructure, and systems allowing for 'Alliance and Member States' societies to continue functioning under conditions of a wide spectrum of threats and hazards: from natural disasters to cyber-attacks, from hybrid to armed attacks. This is an ability to withstand a shock and to be ready for surprises. According to the expert, NATO baseline requirements play an important role in setting the resilience standards that Allies should meet, and resilience is an important part of the NATO-2030 initiative to reform the Alliance (Tarry, 2021).

NATO document "NATO – 2030: a Transatlantic Agenda for the Future" (NATO, 2021c) indicates that resilience is the first line of defense and has major importance for NATO`s success in delivering its three core tasks: collective defense, crisis management and cooperative security.

Analyzing NATO official documents, one can conclude that recommendations provided by this organization on matters of enhancing resilience are often interpreted in the context of strengthening mostly defense capabilities and crisis management including through the concept of total/comprehensive defense that include engagement of all civilian, military, public and private institutions, clear distribution of responsibilities and proper

coordination of actions before, during and after a crisis event in a time of peace and war. It is emphasized also by Lasconjarias (2017).

According to Hodicky et al. (2020), the current NATO approach focuses on the resilience through a civil preparedness in the context of the baseline requirements, namely: how the individual and collective capacity allows for withstanding and recovery from military, civilian, economic, or commercial shocks, absorbing damage, and resuming function as quickly and efficiently as possible.

As the COVID-19 pandemic response demonstrates, crisis management development is an important but not exceptional element to build up national resilience. Thus, seven NATO baseline requirements concerning resilience deal, first of all, with ensuring civilian preparedness, include an ability to handle a big number of victims (NATO, 2016b). In spite of that, most of the Alliance Member States, while having quite well developed crisis management systems, initially faced significant difficulties in countering the COVID-19 spread including difficulties in providing treatment and hospitalization of a big number of patients, continuous supplies of basic commodities, etc. At the same time, according to the opinion of the United Nations Conference on Trade and Development [UNCTAD] (2020), one of the major problems for many countries of the world was the development of a full-scale economic crisis resulting from the implementation of serious restrictions under quarantine and discontinuity of important business processes.

The situation with the spread of COVID-19 revealed that many countries of the world are poorly prepared to respond to a threat of a large scale pandemic and demonstrated flaws in the national systems of crisis management, as well as the presence of significant vulnerabilities in various spheres, first of all, health care and biosafety (Reznikova, 2020b). It should be noted that assessments of the scale threat of the COVID-19 spread and of consequences of the implementation of restrictive quarantine measures, as well as sets of

measures taken in various countries, varied significantly. Some countries, in addition to civilian services engaged in the implementation of quarantine measures also the military, which, in general, meets the total/comprehensive defense principle applied quite widely in the NATO Member States. The Corona-crisis triggered discussions inside the Alliance on whether the NATO baseline requirements for resilience should be specified or expanded

3.1.2. NATO Basic Requirements for National Resilience

Commitment to enhance resilience approved by the Heads of State and Government at the NATO Warsaw Summit in 2016 defined seven baseline requirements (main areas) of strengthening resilience which call for ensuring:

- continuity of government and critical government services;
- resilient energy supply;
- ability to deal efficiently with uncontrolled movement of people;
- resilient water and food resources supply;
- ability to deal with mass causalities;
- resilient civil communications systems;
- resilient civilian transportation systems (NATO, 2016b).

According to NATO (2021b), in 2017, the baseline requirements were used to develop criteria for the national resilience self-assessment by the Member States. Starting from 2018, NATO has been conducting assessments of the Alliance's general resilience every two years. The resulting scores are the basis to identify areas of NATO's further efforts and to support Members in the enhancement of their preparedness in the identified areas. In 2019, NATO leaders recognized the need to enhance the resilience of the societies, as well as of critical infrastructure and energy security of NATO Member States. Additional commitments were undertaken to increase the security of communications including 5G. In 2020, NATO took measures required to prevent the military activities from fostering the spread of COVID-19. Based on

lessons learned from COVID-19 pandemics and other challenges, in particular, those related to new technologies and climate change, NATO continues working on enhancement of resilience of the Member States and their societies (NATO, 2021b).

It should be noted that identification of specific resilience ensuring areas related to the society and critical infrastructure is an important and logical step because these objects are different by their nature. Here, society cannot be viewed as an object of the critical infrastructure but still can be resilient (or not resilient) to threats of different kinds. Clear identification of the objects helps formulating effective means and methods to enhance their resilience with consideration of their specificity. Development of methodological and practical recommendations to ensure resilience in various spheres needs to incorporate the regularities of implementation of the resilience concept in the national security sector, lessons learned from the experience of past events, as well as the context of today's security situation and prospects of its evolution.

According to the Director of NATO Defense Policy and Capabilities Directorate Tarry (2021), Partner States use NATO baseline requirements on resilience to assess the level of their national resilience. With Alliance's support, Member States and Partner States can share their experience and help each other in the risk assessment and lessons learning, formulate their plans and invest in enhancement of their readiness. It should be noted that Ukraine belongs to NATO Partners, which also participate in the national resilience assessments and other joint activities with NATO in this sphere.

Now the Alliance continues to define the agreed requirements, procedures, and criteria to assess national resilience. Experts note that although this is a matter of national responsibility, such a process is based upon values shared by the Member States and their Partners: respect for principles of individual freedom, democracy, human rights, and rule of law (Roepke & Thankey, 2019). Upon approval of the seven baseline requirements for resilience

by NATO Warsaw Summit, the process of assessment criteria improvement runs continuously. At the moment, the main method is development of self-assessment questionnaires.

The ability of a state to provide effective governance and critical government services, especially during a crisis, has a decisive role in the national security under current conditions of major uncertainty and vulnerability. In order to further develop the decisions made at Warsaw (Poland) Summit on 21-22 September 2016, a seminar "Achieving the NATO Baseline Requirement for Continuity of Government" was conducted for representatives of public authorities and experts from the NATO Member States and Partners. Among the main directions of ensuring continuity of public governance, the following ones were specified:

- ability to make, explain, and implement decisions;
- the requirement to execute decisions in a lawful, efficient, and accountable manner even under crisis conditions.

It was also stressed that the reduction of the risks of chaos and disorganization in a society in crisis is facilitated by not only a well-organized and legally adjusted public governance system, first of all in the national security domain, but also by a timely implemented package of measures aimed at protecting this system against consequences of terrorist and informational threats, cyber-attacks, natural disasters, hostile external challenges, etc., as well as an effective interagency interaction (NATO, 2016a).

As of the moment, certain guidelines and recommendations have been developed with respect to each baseline requirement for resilience. In particular, concerning the matters of *ensuring continuity of government and critical government services*, recommendations are contained in the document "Planning Framework for Nations on Assured Continuity of Government and Critical Government Services", AC/98- D(2019)0010(INV).

Important information concerning *resilient energy supply* is contained, in particular, in the following NATO documents: Guidance for National Authorities to Identify and Assess Critical National Infrastructure Resilience and Interdependencies in the Communications and Energy Sectors, AC/98-D(2019)0009 (INV); Guidance on Improving Resilience of National and Cross-Border Energy Networks, AC/98- D(2017)0005-REV1; Recommendations and Best Practices on the Protection of Electricity, Gas and Oil Critical Infrastructure, AC/331-D(2017)0001.

In the area of *ensuring the ability to deal effectively with uncontrolled movement of people*, the following NATO documents deserve attention: Policy on Civil Preparedness for Population Movements in Crisis and Collective Defense, PO(2017)0013; Planning Guidance for Nations on Population Movements, AC/98-D(2019)0011 (INV).

Detailed information with regard to the *resilient food and water resources* is provided, in particular, in the following NATO documents: Guidance on Security of Supply Arrangements for Food and Water Resources, AC/98-D(2019)0005-REV1; Guidance to National Authorities on Managed Supply and Allocation Arrangements, AC/98-D(2019)0004; Planning Guidance to National Authorities' to Mitigate Identified Risks and Vulnerabilities in the Food and Water Sectors, AC/98-D(2017)0002-REV1; Checklist for National Authorities to Mitigate Identified Risks and Vulnerabilities in the Food and Water Sectors, AC/98-D(2018)0004-REV1.

In the area of the *ensuring the ability to deal with mass casualties,* the following NATO documents should be noted: Guidance to National Authorities for Planning for Incidents Involving Catastrophic Mass Casualties, AC/98-D(2018)0002-REV1, multiref; Guidance to National Authorities for a Robust Security of Supply and Supply Chain Arrangements, AC/98-D(2019)0003-REV1, multiref; Non-Binding Guidelines for Enhanced Civil-Military

Cooperation to Deal with the Consequences of Large-Scale CBRN Events[4] Associated with Terrorist Attacks, PO(2019)0054.

Important information with regard to the *resilient civil communications systems* is dealt with, for example, in the following NATO documents: Guidance on the Development of Priority Arrangements for Civil Telecommunications, AC/98-D(2017)0004-REV1.

Recommendations and guidance in the area of the *resilient civil transportation systems* are contained in the following NATO documents: Guidance on Single National Points Of Contact, AC/98-N(2018)0006; Guidance to Assist Allies in Establishing Legislation/Standards for Strengthening Transport Infrastructure and Development of Operational Protocols to Deny/Limit Access to Transportation Resources, AC/98- N(2017)0055-REV1.

In 2021, the baseline requirements for national resilience and appropriate recommendations were significantly deepened. The Brussels NATO Summit Communique as of 14 June 2021 states, inter alia, that the resilience has a major significance for reliable deterrence and defense and for the effective execution of the Alliance's main objectives. NATO confirmed its adherence to the application of the whole-of-government approach to enhancement of resilience of the Member States and their societies and to achievement of NATO`s seven baseline requirements for national resilience through strengthening of civil-military cooperation and civil preparedness, tighter interaction with the population, private sector, and non-governmental actors, as well as through the centres of expertise on resilience established by Allies. Alliance's resilience will be enhanced also thanks to the deepening of cooperation with Partners and other international organizations (NATO, 2021a).

The aforementioned Communique emphasizes the importance of counteracting hybrid threats. It notes that in cases of a hybrid war, it can be

[4] A CBRN event means results of the use of chemical, biological, radiological, or nuclear weapon

decided to induce Article 5 of the Washington Treaty similarly to a case of an armed attack. NATO and Allies continue preparing for, deter and defend against hybrid threats including by increasing their situational awareness and expanding means to counteract hybrid threats through developing comprehensive options for prevention and response (NATO, 2021a).

During Brussels NATO Summit (2021), the Strengthened Resilience Commitment was approved, which defines further steps to be implemented as soon as possible. The purpose of such activities was defined as reducing vulnerabilities and making sure that the Alliance troops are capable of operating effectively in peace, crisis, and conflict time. According to these documents, Member States have to formulate proposals on the establishment, evaluation, revision, and monitoring of resilience goals and plans for their implementation at the national level (NATO, 2021e).

The NATO Strengthened Resilience Commitment also noted that threats and challenges to NATO's and Member States' resilience can be originated from both state and non-state actors, have different forms, and involve the use of various tactics and tools which include: conventional, non-conventional, and hybrid threats and activities; terrorist attacks; sophisticated malicious cyber activities; hostile information activities, including disinformation, aimed at destabilizing our societies and undermining our shared values; and attempts to interfere with democratic processes and good governance. NATO's and Member States' activities to enhance resilience will have, in particular, such objectives as securing and diversifying supply chains; ensuring the resilience of critical infrastructure (on land, at sea, in space, and in cyberspace) and of key sectors, such as: protecting them from harmful economic activities; securing against threats stipulated by the impact of emerging technologies; securing next-generation communications systems, technologies, and intellectual property; ensuring energy security and mitigation of consequences of natural hazards that

which are being exacerbated by climate change become more robust due to climate change (NATO, 2021e).

Speaking at Bratislava Global Security Forum GLOBSEC 2021, NATO Deputy Secretary General M. Geoană noted that the new NATO resilience commitment interprets the respective domain of activity wider than before. In particular, it includes response to the climate change consequences, risks for critical infrastructure, supply chains, telecommunications or risks related to direct foreign investments. At the same time, the official noted that such an approach never leaves out any other important issues of hard security. Now NATO works on countering hybrid threats, as well as threats in cyber domain, space, or from China, Russia, and other countries including competition for raw materials important for microchip production. Also, Bratislava forum underlined the importance of the clear distribution of responsibilities for deepening cooperation between the EU and NATO in matters of strengthening resilience (GLOBSEC Bratislava forum, 2021).

NATO plans for the future include expanding and coordinating approaches to resilience enhancement through better definition of goals with respective criteria and indicators which need to be flexible enough, thus allowing for their adaptation to the national conditions. This will help to improve monitoring and assessment by NATO, preparing recommendations for the Member States with respect to national resilience enhancement according to the collective defense needs (NATO, 2021c).

So, gradual change is observed in NATO's approach to the resilience through expansion of areas of civil-military interaction and greater attention to matters of societal resilience. Respective NATO practices, in parallel, implement in general the basic principles of the resilience concept in the security domain with regard to the ability of the Alliance, its Members and Partners to adapt their policies to conditions of uncertainty, to timely identify and eliminate vulnerabilities, to develop respective capabilities and interaction, etc.

3.2. EU Conceptual Approaches to Development of Resilience of the Union and its Member States

3.2.1. Changes in EU Strategic and Program Documents on Resilience of the European Union and its Member States

For quite a long time, issues of resilience in the EU had been viewed mostly in the context of achievement of Sustainable Development Goals (before 2015, Millennium Development Goals) while the key activities had been aimed at building resilience of the states beyond the EU boundaries to emergencies and crises associated with climate change, natural and man-made disasters, etc. (United Nations [UN] General Assembly, 2000, 2015).

Key approaches to the EU resilience were presented, in particular, in a number of documents, among which the following should be mentioned: Council Conclusions on EU Approach to Resilience, Communication from the Commission to the European Parliament and the Council on EU approach to resilience: learning from food security crises, as well as European Commission's papers: The EU Approach to Resilience: Learning from Food Security Crises, Building resilience: the EU's approach, and others (Council of the European Union, 2013; European Commission, 2012, 2014a, 2014b, 2016b). Analyzing these documents, it could be assumed that at the moment of their preparation and adoption, the following considerations were at the basis of the EU strategic approach to resilience:

- When periodicity and intensity of emergencies and humanitarian crises grow, their impact on the developing nations is the main threat to their long-term development. Hence, it is really necessary to help the people and states withstand significant shocks and recover, in other words, enhance their resilience. Investing in resilience costs less than responding to crises afterward;

- Main attention should be focused on vulnerabilities and removal of major causes of the crises (especially chronic poverty) rather than on their consequences. To do this, appropriate state policy needs to be developed, which covers several components: risk assessment; measures to reduce the risk, prevent it, mitigate its consequences, and provide preparedness; enhancement of capabilities of prompt crisis response and recovery;
- EU priorities in ensuring resilience: mitigation of potential consequences of natural and man-made disasters, as well as coping with crisis situations in fragile or conflict-affected states. Different situational contexts require differentiated and goal-oriented approaches.

In general, the EU resilience was defined as the ability of an individual, a household, a community, a country, or a region to prepare for, withstand, adapt, and quickly recover from stresses and shocks such as natural and man-made disasters without compromising long-term development prospects. There were official documents defining guidelines of the EU support to building resilience in partner states, as well as establishing that the resilience development and identification of respective political, economic, and environmental priorities are national responsibilities (Council of the European Union, 2013; European Commission, 2014a, 2014b, 2016b; European Parliament, 2017).

In 2012, the EU launched two main resilience initiatives: Supporting Horn of African Resilience [SHARE] and l'Alliance Globale pour l'Initiative Résilience – Sahel et Afrique de l'Ouest [AGIR]. Analysis of the EU official documents gives grounds to affirm that the main priorities of the EU support of building resilience in developing states are the following: adaptation to climate change, reduction of emergency risks, support to agriculture, food security and social protection, poverty reduction, providing access to medical and educational services, etc. (Council of the European Union, 2013; European Commission,

2014a, 2014b, 2016b; European Parliament, 2017). In the humanitarian assistance, the EU introduced the "resilience marker": all humanitarian projects had to include options to reduce future risks, strengthen coping capacities to avoid or reduce future humanitarian needs (European Commission, 2016b).

In the context of formulation of the EU security and domestic policy, the matters of resilience, as a rule, had not been raised before. For instance, there are no references to the resilience in the European Security Strategy "Secure Europe in a Better World" (Council of the European Union, 2003).

Changes that have occurred in the global security environment, especially after 2014, have shown that the number of threats faced by the European Union and its members increased. Hence, the EU needed to revise its approaches to its foreign and domestic policy making. The matters of resilience of both the EU Member States and the states located to the east and south of the EU became one of the priorities identified by the European Union's global strategy for foreign and security policy "Shared Vision, Shared Action: Stronger Europe" (Global Strategy) (European Union, 2016). The reason for that was that now issues of domestic and external security overlap every time more frequently.

Now the EU vision of resilience is based on the ability of the Member States and the Union, in general, to resist a wide spectrum of threats without losing the shared democratic values. The EU views sustainable development, economic stability, good governance and protection of human rights as the key conditions for ensuring national resilience.

The EU Global Strategy, in particular, refers to the following main directions and objectives for enhancing the resilience of the states and their societies in both the EU and the whole of Europe:

- promoting the resilience of the Member States according to the shared values (respect for and promotion of human rights, main freedoms, rule of law, justices, solidarity, equality, non-discrimination, pluralism, and respect for variety);

- enhancing resilience of critical infrastructure, networks and service in cyber-space;
- enhancing societal resilience, in particular, through deeper relations with the civil society, cultural organizations, religious communities, social partners, etc.;
- investing in the resilience of states and societies located east (to Central Asia) and south (to Central Africa) of the EU, in particular, the EU's closest neighbors and states of origin and transit of migrants and refugees;
- enhancing energy and environmental resilience (European Union, 2016).

Also, the EU Global Strategy defines a resilient state as a secure state, and security as a foundation for prosperity and democracy. Still, to ensure sustainable security, it is not only state institutions that need to be supported. The document outlines transition to a wider approach: understanding resilience as a notion embracing all the people and the whole society because a resilient democratic society featuring democracy, trust in institutions, and sustainable development lies at the heart of a resilient state (European Union, 2016).

At the same time, the document establishes that the goal-oriented approaches to the resilience, prevention and resolution of conflicts within the EU boundaries and beyond require a deeper situational awareness while the crises needs to be responded to, first of all, on the basis of Common Security and Defense Policy, humanitarian assistance, sanctions, and diplomacy. In this context, resilience is defined as the ability of states and societies to reform in order to withstand and recover successfully from internal or external crises (European Union, 2016).

With the adoption of the EU Global Strategy, a strategic approach to resilience in external actions was specified. European Parliament and the

Council (2017) note that the objectives for the EU's external action in the development of resilience are to strengthen:

- adaptability of states, societies, communities, and individuals to political, economic, environmental, demographic, or social pressure in order to achieve stability in the implementation of the national development goals;
- capacity of states, under intensive pressure, to implement, maintain or restore the main functions, social and political cohesion in a manner, which ensures democracy, rule of law, human rights and fosters national security and progress in a long-term prospect;
- capacity of societies, communities, and individuals to manage opportunities and risks in a peaceful and stable manner, as well as to ensure, maintain or restore livelihoods under intensive pressure.

The aforementioned document deals with the EU's support for strengthening the resilience of a state, society, and communities in partner states. Various resilience ensuring areas are considered including economic, social, environmental resilience, etc.

Thus, now the EU uses the notion of resilience in the context of state-building, good governance, ensuring security and human rights, and sustainable development in both the EU and the Partner States. Since 2014, efforts have been applied to strengthen the security component of the EU activity, and also there has been a trend towards expansion of the EU's cooperation with NATO and OSCE, first of all, in order to counter hybrid threats. Thus, the Joint declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization (2016) was signed, which dealt, in particular, with the need to join efforts countering new challenges and hybrid threats. In 2017, the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) was founded

in Helsinki, Finland[5]. This is an international organization, that brings together 31 EU and/or NATO Member States. Its activities are aimed at strengthening the EU's and NATO's capabilities to prevent and counter hybrid threats.

In view of the increase of volatility and uncertainty in the global security environment, as well as with consideration of the expansion of hybrid threats, the EU states are increasingly raising the issue of expanding the areas of building national and regional resilience. European Parliament and the Council (2016) defined the main goals and objectives of countering hybrid threats in the EU Member States, in particular:

- to recognize the hybrid nature of a threats;
- to organize respond to hybrid threats;
- to build-up the resilience;
- crisis prevention, response, and recovery;
- to increase cooperation with NATO.

This Joint Communication points out that the hybrid threats are aimed at exploiting vulnerabilities of state and society and to undermine fundamental democratic values and liberties (European Parliament and the Council, 2016). To increase the situational awareness it is appropriate to monitor and to assess the risks that can target the EU's vulnerability. It was deemed necessary to develop security risk assessment methodologies in many areas: from aviation security to terrorist financing and money laundering. Also, it was suggested to conduct a survey in the Member States identifying areas vulnerable to hybrid threats in order to identify indicators thereof, which could be incorporated into early warning and risk assessment mechanisms. It was suggested to the Member States to conduct a study of the hybrid risks to identify the key vulnerabilities, first of all, of the national and pan-European structures and networks (European Parliament and the Council, 2016).

[5] *The European Centre of Excellence for Countering Hybrid Threats.* https://www.hybridcoe.fi/about-us/

In the context of creation of the EU mechanism to respond to hybrid threats, the Member States were invited to establish National Contact Points on hybrid threats to ensure cooperation and secure communication with the respective EU entities. Also, it was deemed necessary to update and coordinate capacities to deliver proactive strategic communications (European Parliament and the Council, 2016).

The aforementioned Joint Communication identified the following key areas of building resilience:

- protection of critical infrastructure (first of all, energy supply, transport and other supply chains and satellite communications);
- development of defense capabilities;
- protection of public health and food security;
- ensuring cyber security;
- preventing the hybrid threat financing;
- countering radicalization and violent extremism;
- development of cooperation with the partner countries (European Parliament and the Council, 2016).

In November 2016, a High Representative of the Union for Foreign Affairs and Security Policy, Vice President of the European Commission Federica Mogherini presented Implementation Plan on Security and Defense, which was approved by the European Council in December of the same year. The document determined three strategic priorities in the EU activities in security and defense:

- response to external conflicts and crises;
- building the capacities of partners;
- protection of the Union and its citizens (Council of the European Union, 2016).

Due to this document, the key activities included, in particular, the following: deepening of defense cooperation including establishment, starting from 2017, of the Coordinated Annual Review on Defense (CARD); revision of the Capability Development Plan (CDP); development of Permanent Structured Cooperation, PESCO to enhance defense capacity and civilian capabilities of the EU Member States; adjustment of the EU's rapid response toolbox; establishment of Military Planning and Conduct Capability (MPCC) in addition to the existing structure - Civilian Planning and Conduct Capability (CPCC); development of partnership within the EU Common Foreign and Security Policy including assisting partners in development of national resilience and respective capabilities (Council of the European Union, 2016).

In addition to deepening the cooperation between militaries and civilians, the EU also pays a great deal of attention to the establishment of constructive relations between state and private actors, first of all, owners of the critical infrastructure facilities. Still, the existing mechanisms require improvement. Roepke and Thankey (2019) underline that national public authorities have legislative and regulatory powers but very few direct controls to influence or steer supply in the private/commercial sector, other than in an emergency situation; governments pay their main attention to safety and quality of goods and services, especially food products. The researchers note that the EU plays a very important role in the public administration architecture for these sectors. In particular, the EU directives and regulations establish requirements for emergency planning applicable not only to the Member States governments but also to the commercial sector. At the same time, Roepke and Thankey (2019) note that until recently, issues of ensuring security and defense in the context of protection of supply chains and infrastructure in crises have not been deemed important. According to these authors' opinions, the established mechanisms and procedures were designed mainly for extreme situations, such as war, but

not for conflicts, for instance, of the hybrid type, that would accompany an escalating geopolitical crisis short of outright armed conflict.

The EU now continues developing and implementing documents that regulate various aspects of comprehensive counteraction to the newest threats by the EU. In particular, the key goals and objectives of the EU to fight disinformation have been defined (European Commission, 2018). Overall, there is a visible trend toward strengthening the security component of the EU policy in the background of growth of instability and spread of new challenges and threats.

The fight against the CODIV-19 pandemic raised new issues with respect to crisis response and recovery in the EU. The European Council (2020a) calls for shaping a coordinated strategy for exit from the CODIV-19 crisis and comprehensive recovery and investment plan. Later on, an innovative tool for provision of support to the Member States and provide direct financial support to the Member States through the Recovery and Resilience Facility was developed and the respective Regulation on it was approved by the European Commission and agreed upon with European Parliament and Council on December 2020, while the final approval thereof took place on February 2021 (Council of the European Union, 2020; European Parliament and Council, 2021a). Within this Facility, the financial assistance fund was formed to be used to extend loans and grants worth 672.5 billion euros to the EU Member States in support of reforms aimed at the post-crisis recovery and strengthening of the national resilience. The EU Member States are expected to deliver the recovery and resilience plans which would shape the national reform package and the intended governmental investments. To use this Facility-based support, such investments have to be made by 2026 (European Commission, 2021).

The Recovery and Resilience Facility is an integral part of the EU economy promotion program after COVD-19 named Next Generation EU[6]. This Program is a package of temporary measures of financial support to the EU Member States, which is aimed at both immediate compensation for negative economic and social consequences caused by the crisis and achievement of long-term objectives of the EU development, in particular, with respect to adaptation to climate change, economy digitalization, increase of the resilience and effective response to the current and future challenges. The Program is expected to become an economic booster for research and innovation in the area of future technologies (in particular, 5G new generation telecommunication deployment, development of networking infrastructures, artificial intelligence, digitalization of industry, renewable energy, environment-friendly transport, energy-efficient buildings, etc.), to foster modernization and acceleration of the EU economic development pace. Besides, the allocated funds will allow for implementing the immediate structural reforms required to increase the EU resilience.

The Road Map for recovery "Towards a more resilient, sustainable and fair Europe" was developed (European Council, 2020b). In addition to the economy promotion measures, this document also reads that the key condition to overcome the crisis and recover is a functioning system of governance. It means in practice:

- ensuring the EU resilience through drawing the lessons learned during the crisis, active cooperation of all of the EU Member States with strict compliance with the principle of subsidiarity;
- ensuring the EU efficiency through development of the executing capabilities and enhancement of the coordinated crisis management;

[6] *Recovery plan for Europe.* Recovery plan for Europe, https://ec.europa.eu/info/strategy/recovery-plan-europe_en

- protection of the EU basic values (respect for the rule of law and human dignity) as the best way to ensure a solid and comprehensive recovery of the society (European Council, 2020b).

Resilience enhancement is defined as the main goal of the EU Eastern Partnership Policy. The respective goals were stated in the Joint Declaration of the Eastern Partnership Summit that took place in December 2021 "Recovery, Resilience and Reform"[7]. This document reiterated unchangeable EU's aspirations to build an area of democracy, prosperity, stability, and enhancement of cooperation with the Partner States on the basis of shared values, first of all, respect for democracy, basic human rights and freedoms. The aforementioned Declaration states a number of goals aimed at Partner States' resilience enhancement and foresee implementation or deepening of certain reforms by them. These political goals are structured into two groups:

1) Governance: accountable institutions, rule of law and security; resilient, gender-equal, fair and inclusive societies; strategic communications;

2) Investments: resilient, sustainable, and integrated economy; environmental and climate resilience; resilient digital transformations.

The Declaration states the following priority directions for deepening the cooperation and implementation of reforms in order to enhance resilience, development, and prosperity:

- support for the rule of law, establishment of efficient, transparent, and accountable public governance at all levels;
- reform of justice and protection of human rights;
- fight against corruption, economic crimes, fraud, and organized crime;

[7] Council of the European Union. *Joint Declaration of the Eastern Partnership Summit "Recovery, Resilience and Reform".* Brussels, 15 December 2021. https://euneighbourseast.eu/wp-content/uploads/2021/12/20211215-eap-joint-declaration-en.pdf

- acceleration of digital transformation through investments into digital infrastructure and E-Governance; ensuring cyber-resilience including to hybrid threats; prospective creation of a common international roaming space, reduction of roaming tariffs between the EU and Eastern Partners;
- development of cooperation between the EU and Eastern Partners in the area of fight against disinformation and information manipulations; strengthening of support to independent mass media;
- strengthening of democracy, development of civil society and inclusion of youth, promotion of gender equality, reform of education;
- development of the health care system, enhancement of anti-epidemic resilience;
- ensuring sustainable and reasonable mobility through facilitation of the legal and labor mobility and counteraction to illegal migration;
- enhancement of economic resilience through promotion of commercial and economic integration, incentives to invest, facilitation of access to finances, improvement of transport connections, and investment in human capital and knowledge development;
- enhancement of environmental and climatic resilience through enhancement of "green" and digital transformations, support to investments and strengthening of cooperation for adaptation to the climate change and enhancement of bio-variety; ensuring climatic neutrality by 2050 through gradual rejection of coal; reductions of the carbon trace and further enhancement of inclusive sustainable development in the energy sector;

- prevention of use of the natural gas as a weapon or geopolitical leverage, enhancement of nuclear safety, etc.

The political goals stated in the document will be consolidated with an economic and investment plan containing the defined national initiatives to be implemented with each one of the Partner States with financial support from the European Union (total amount of 2.3 billion euros with potential mobilization of up to 17 billion euros through governmental and private investments).

Hence, the EU measures aimed at overcoming the crisis caused by the COVID-19 pandemics and ensuring further development are mostly aimed at enhancement of the EU resilience in various spheres, as well as that of the Member States, the Partner States, and their societies. The suggested approaches embody such features of the resilience concept in the security field as movement (in the form of ability of the EU Member States and the Partner States to reform and enhance capabilities) and immutability (maintaining the basic EU principles and values).

3.2.2. Organization of Civil Defense and Emergency Response System in the EU Member States

In the context of the national resilience development, the EU States pay a great deal of attention to ensuring preparedness and emergency risk management in the civil defense sector (Reznikova et al., 2021). It is called forth by the fact that most emergencies cannot be avoided (especially those of natural origin) but their negative impact on the society and state can be reduced. Taking into consideration that the primary response to threats and crises has to take place directly where they occur, organization of the civil defense and ensuring preparedness to respond to crises and threats at the regional and local levels have major importance. An important role in the security and resilience ensuring systems in local communities of the EU Member States belongs to the local and territorial authorities. A procedure of interaction of various resilience actors and

implementation of the threat response measures is regulated not only by the national legislation but also by the legislation of the EU as well as by the international treaties.

In particular, an important role in regulation of relations in the aforementioned area belongs to the Sendai Framework for Disaster Risk Reduction 2015-2030 (United Nations, 2015a). The European Union undertook the leading role in negotiating it and supports all of the states (both EU Members and non-members) in their aspiration to achieve the established targets.

In June 2016, European Commission adopted Action Plan on the Sendai Framework for Disaster Risk Reduction and established the respective financial facilities (European Commission, 2016a). Measures included in the Action Plan have to be implemented in the EU States at all levels and provide, in particular, for collection and sharing of data on losses caused by emergencies, exchange of experience, promotion of partnerships between the public and private sectors in the matters of risk management, development of infrastructure in the cities, implementation of governmental programs for risk management, and creation of the required capabilities.

Local and regional authorities of a number of the EU states are legally and politically responsible for the protection of the population. As a rule, they are the first public governance level in the area of natural disaster response. Implementation of the Sendai Framework at the EU level contributes to successful achievement of the risk reduction and capability development goals for mitigation of the emergency impact by the local and regional authorities.

Besides, the EU has its Civil Protection Mechanism. According to article 214 of the Lisbon Treaty, the EU has a number of obligations concerning protection of and assistance to casualties of natural and man-made disasters all around the world. The Treaty provides support and coordination of the Member States' civil protection systems (art. 196), as well as empowers the EU institutions to decide on the measures required to do so (European Union, 2007).

Certain issues of functioning of the aforementioned Mechanism are defined by the Resolution of European Parliament and Council No 1313/2013/EU of 17 December 2013, on EU Civil Protection Mechanism (European Parliament and Council, 2013).

Regulation of European Council No 2016/369 of 15 March 2016, on the provision of emergency support within the Union; European Parliament and Council Regulation No 2021/888 establishing the European Solidarity Corps of 20 May 2021; Council Regulation concerning humanitarian aid No 1257/96 of 20 June 1996, and others (European Council, 1996, 2016; European Parliament and Council, 2021b) deserve mention among other documents regulating the interaction of the EU states in civil protection and respective assistance.

The main institutional structure of the EU Civil Protection Mechanism is the Emergency Response Coordination Centre [ERCC]. It coordinates issues of assistance to the countries affected by emergencies, in particular, concerning allocation of material resources and special equipment, experts' analysis, establishment and conducting the civil protection groups. The Center harmonizes interaction among all EU Member States, six more countries-participants in the Mechanism, the United Kingdom, the victim country, and experts in civil protection and humanitarian matters. The Center operates 24/7 and can extend assistance to any country within or beyond the EU in the case of a large-scale disaster at requests of the national authorities or UN authorized body.

The concerted response to man-made disasters and natural hazards at the European level allows for avoiding an overlap of assisting efforts and for ensuring that such assistance meets the needs of the affected parties. Emergency Response Coordination Center can contact directly national civil protection authorities of a country needing assistance and provides financial support to transport the civil protection assets to the affected country.

Emergency Response Coordination Center has its own portal[8] where there is a detailed description of its activities and other appropriate information. In particular, the Portal offers the Vademecum[9] as a source of information for professionals working in civil protection at national, regional, and local levels, volunteers, non-governmental organizations, and representatives of the public. It contains information on the civil protection organization and a general overview of measures taken by the Mechanism Member States and at the EU level to respond to emergencies and mitigate their impact that can be caused by natural disasters, such as earthquakes, landslides, forest fires, floods, droughts, snow storms, tidal waves and/or by human activities, for example, large-scale accidents (including industrial, in particular, chemical accidents), social disturbances, terrorism, etc.

Thus, the EU activities in emergency risk management and civil protection are organized according to the principle of subsidiarity and wide interaction, which are the key ones to ensuring the national resilience. Now, many EU countries practice the overarching systems approach to providing preparedness and response to wide spectrum of threats, according to which, the issues of civil protection of the public and crisis management are viewed as a united whole with other aspects of ensuring national security and resilience.

Overall, the EU conceptual approach to ensuring resilience features some changes to the side of increasing efforts to enhance the resilience of the Union and its Member States rather than of external actions and help to the developing countries. Also, there have been some changes concerning the consolidation of the defense and security components of the EU policy simultaneously with further development of the crisis management and ensuring sustainable development.

[8] *Emergency Response Coordination Centre.* https://erccportal.jrc.ec.europa.eu/
[9] *Vademecum – Civil Protection home.* https://erccportal.jrc.ec.europa.eu/vademecum/index.html

3.3. Recommendations of UN, OECD, and other International Organizations with regard to Building National Resilience

3.3.1. Sustainable Development and Resilience in UN

In the modern world, the ensuring of sustainable development is often pinpointed by development of resilience in the key sectors of economy and societal relations. With consideration of the approaches to the sustainable development concept adopted at the UN level, its main components are economic growth, social inclusion, and environmental protection (UN General Assembly, 2015). At the same time, sustainable development is impossible without ensuring peace and security and without productive cooperation at the international level (Reznikova, 2019a). This is confirmed, in particular, by the choice of UN basic priorities, which have critical importance for further development, namely: humans, planet, prosperity, peace, and partnership. They were defined in the UN General Assembly Resolution "Transforming Our World: The 2030 Agenda for Sustainable Development" (UN General Assembly, 2015).

Links between resilience and sustainable development are embodied in the current strategic documents of the leading states and their alliances. In particular, the EU Global Strategy features a trend to view resilience through the prism of sustainable development (European Union, 2016).

The UN goals and objectives defining the course of actions of the states and international organizations in the sustainable development and security domains are of major importance. In 2000, at the UN Summit 189 States adopted the Millennium Declaration approved by the Resolution of the UN General Assembly (UN General Assembly, 2000). This document defined eight millennium development goals as a global framework of values, principles, and key factors of development until 2015, namely: eradicate extreme poverty and

hunger; achieve universal primary education; promote gender equality and empower women; reduce child mortality; improve maternal health; combat HIV/AIDS, malaria and other diseases; ensure environmental sustainability; global partnership for development. All the goals and objectives embraced mostly the key domains for sustainable development: economic, humanitarian and environmental.

Upon expiration of the Millennium Goals, in September 2015, within the 70-th UN General Assembly, UN Summit for sustainable development took place in New York, the Agenda for Sustainable Development was defined and 17 Sustainable Development Goals [SDG] and 169 objectives, in order to achieve the goals, were approved (UN General Assembly, 2015). The approved goals and objectives are aimed at solution of many problems in various domains: social, economic, humanitarian, energy, environmental, security and other. Comparing the Sustainable Development Goals with the Millennium Challenge Goals, it should be noted that the list of spheres and objectives is much wider in the new document. As stated in the UN General Assembly Resolution "Transforming Our World: The 2030 Agenda for Sustainable Development", the UN Member States undertook ambitious obligations concerning the global transition to a resilient and stable path of development (UN General Assembly, 2015).

Analyzing goals and objectives for sustainable development identified by the UN documents one can conclude that they contribute to the enhancement of the national resilience including improvement of the crisis management because they define, among other aspects, a number of activities to enhance resilience of energy supply and transport systems, as well as eliminate roots for any tensions in a society.

Sustainable development goals establish landmarks for policy-making, as well as for funding in the appropriate areas of activities of the UN Development Program [UNDP], which is the key UN agency for sustainable development

issues and supports national governments in adaptation and implementation of SDG. Other UN institutions and organizations (in particular, World Bank, World Health Organization [WHO], International Labor Organization [ILO], UN Food and Agriculture Organization [FAO], UN Children Fund [UNICEF], "UN-Women" Program, United Nations Office for Disaster Risk Reduction [UNDRR], and others) are also guided by UN Sustainable Development Goals, generating and implementing programs within the areas of their responsibilities.

In May 2016, the Global Humanitarian Summit was held, which, along the same lines of The 2030 Agenda for Sustainable Development, established Agenda for Humanity (United Nations, n.d.). The document identifies five main lines of activities:

- global leadership to prevent and end conflicts, which includes political solutions, unity of goals, stability of governance, and investment in peaceful societal development;
- uphold the norms that safeguard the humanity, which envisages minimizing human suffering and protecting civilians through compliance with and strengthening of provisions of the international law;
- leaving no one behind, which means giving assistance to all in cases of conflicts, emergencies, vulnerabilities and risks;
- changing people's life: from delivering aid to ending need, which envisages reinforcing local systems, anticipating and bridging gaps in the human development;
- investing in humanity.

The activities identified in the document provide a significant potential to enhance the resilience of different states, first of all, those which are developing. In particular, Agenda for Humanity provides the requirement to develop early warning systems, national capabilities to analyze and manage risks, as well as systems of threat prevention and response, implementation of a comprehensive

approach to respond to a wide spectrum of risks and threats, strengthening of civil protection and interaction with the public, etc. (United Nations, n.d.).

Support in reducing the risk of an emergency is an important direction of UN activities in the context of states' resilience enhancement. In particular, during the World Conference held on 14-18 March 2015 in Sendai (Japan), UN Member States adopted Sendai Framework for Disaster Risk Reduction for 2015-2030 (United Nations, 2015a). This global treaty is aimed at enhancement of social and economic resilience through the mitigation of the negative impact of climate change, man-made disasters and natural disasters.

Before the Sendai Platform, the effective documents were Yokohama Strategy for a Safer World, which contained recommendations on emergency prevention, preparedness and mitigation of its impact (United Nations, 1994), and later, Hyogo Framework of Action 2005 – 2015 "Building the Resilience of Nations and Communities to Disasters", which suggested a strategic systemic approach to reduction of vulnerabilities and risk of disasters, and also identified ways to enhance states' and societies' resilience to disasters (United Nations, 2005).

It should be noted that the activities identified by Sendai Framework complement those contained in other international documents. They include, for instance, The 2030 Agenda for Sustainable Development, The Paris Agreement, The Grand Bargain, launched during the World Humanitarian Summit [WHS] in Istanbul (Turkey) in May 2016, New Urban Agenda, the final document of the UN Conference on Housing and Sustainable Urban Development held in October 2016 in Quito (Ecuador), and others (UN General Assembly, 2015, 2016; United Nations, 2015b; WHS, n.d.).

In 2017, the United Nations Plan of Action on Disaster Risk Reduction for Resilience Towards a Risk-informed and Integrated Approach to Sustainable Development was revised and specified (United Nations, 2017). This document is the UN contribution to support the implementation of the Sendai Framework

and promotes the integrated approach to the achievement of objectives of The 2030 Agenda for Sustainable Development.

After changes in the global security environment, in particular, after Russia, as a UN Security Council Permanent Member, launched hybrid aggression against Ukraine in 2014, the UN started paying more attention to the security issues. Thus, in April 2014, UN Security Council Resolution on ensuring global peace and security and the security sector reform was adopted. This document emphasizes, inter alia, the importance of security sector reform for the stabilization and recovering post-conflict states and the addition of respective tasks to UN peacekeeping operations and special political missions (UN Security Council, 2014). It also notes that the security sector reform needs to be in concert with other national political processes including various aspects of societal development like participation of the civil society in political processes and public governance, which lays foundations of stability and peace on the basis of national dialogue and efforts to achieve conciliation and common solutions. It underlines the importance of the security sector comprehensive reform in order to arrange for more effective interaction and integration of police, border guard, defense, maritime security, civil protection, and other forces, as well as for the development of capabilities fostering enhancement of community resilience, as well as institutions responsible for oversight and governance (UN Security Council, 2014).

It should be noted that the measures contributing to the national resilience enhancement are also identified in other UN Security Council resolutions. In particular, the UN Security Council (2017a, 2017b, 2017c) mentions enhancement of resilience to terrorist attacks, which requires, among other things, appropriate measures in the domain of civil protection, ensuring public security, protection of national economy and people's welfare, reliability and resilience of the critical infrastructure. In addition, these documents focus on the need to establish broad expert cooperation on risks and capabilities assessment

issues in the field of counter-terrorism, including involvement of scientific institutions and civil society.

In general, the UN approach to enhancement of the nation's resilience is aimed at removing the causes of their vulnerabilities. In particular, it refers to eradication of hunger, inequality on any basis, the ensuring of appropriate medical and educational services, adaptation to climate change, disaster risk reduction, providing conciliation and trust, etc. According to these priorities, UN institutions develop and implement targeted assistance programs for the states that need them. Among the programs dedicated to various aspects of the resilience enhancement implemented with the support of the UN and its organizations the following deserve mentioning:

- FAO Resilience Programme in Somalia (effective term: 01.11.2014 – 31.10.2015, budget: $1.69 mln.). The purpose is to support beneficiary households and communities diversify income sources and livelihood strategies, increase food production in a sustainable manner or restore productive capacity when faced with chronic pressure or shocks (FAO, n.d.);
- Integrated Project Portfolio on building resilience in response to the Syria crisis (3RP and SRP): total amount was $8.4 mln.; the Portfolio integrated various UN organizations and programs, non-governmental institutions, and other partners. The purpose was to ensure stability in Syria, solve the large-scale problem of refugees from the country, augment the resilience of the neighboring countries, which include enhancement of the national capabilities of Jordan, Lebanon, Turkey, Iraq, and Egypt to mitigate the crisis impact and overcome the crisis (UNDP, n.d.; UNHCR, n.d.);
- City Resilience Profiling Programme, UN Program for urban areas. The purpose was to increase awareness, share knowledge, and

engage in the technical cooperation with the cities in all areas of planning, governance, city functioning, etc. (UN-Habitat, n.d.).

It is also worth mentioning that, as a rule, the states formulate their national resilience strategies and plans with consideration of their obligations due to the treaties and other UN documents.

3.3.2. Projects of OECD and other International Organizations in Building National Resilience

For the ***Organization of Economic Cooperation and Development*** [OECD], resilience means that the states can better withstand environmental, political, economic and social shocks and stresses (OECD, 2014a). This is based on the ability of individuals, communities, and states and their institutions to absorb and recover from shocks, whilst positively adapting and transforming their structures and means for living in the face of long-term changes and uncertainty (OECD, 2013). The matter of building resilience is the focus of the Organization after the global financial crisis of 2008–2009. The main areas of OECD activities with respect to the resilience enhancement are as follows:

- to provide guidelines on how to assess risks together – across policy groups, across donors, with states, and local people – by adapting systems that donors use to assess risks in their own home countries;
- to provide recommendations on the appropriate incentives to ensure that the results of joint risk assessment are used to develop the appropriate policies, strategies and programs to build resilience across the different risk layers;
- to collect and share best practices in strengthening each of the components of resilience;
- to develop guidelines for communicating about risk and outcomes of the resilience programs (OECD, 2013).

Currently, OECD formulates the resilience enhancement action plans with consideration of the goals and objectives identified in The 2030 Agenda for Sustainable Development and Agenda for Humanity (UN General Assembly, 2015; United Nations, n.d.). In particular, OECD defined the following priorities of such activities:

- increasing coherence between humanitarian, development and peace and state-building actions;
- focusing on the most vulnerable states and societies;
- investing in crisis risk management;
- promoting context-specific approaches: in order to better understand the structural drivers of vulnerability and to adequately address them humanitarian, development and peace and state-building actors need to build a common understanding of risks, capacities and vulnerability in a specific context, to inform response, recovery and development plans (OECD, n.d.c).

OECD has already developed a number of recommendations to ensure resilience with respect, in particular, of the following aspects:

- conducting the Resilience Systems Analysis (OECD, 2014a);
- building resilience of the state in fragile situations (OECD, 2008);
- enhancing resilience of economy, society, institutions and environmental resilience (OECD, 2014b);
- enhancing resilience of cities (OECD, 2016), etc.

These recommendations pay a great deal of attention to the matters of risk assessment and organization of the respective activities on the basis of wide cooperation, identification of vulnerabilities of the state and society, development of strategic and program documents with respect to strengthening of the national resilience with consideration of the obtained results of the assessment and analysis. For example, a number of projects were implemented

making use of the Resilience Systems Analysis methodology developed by OECD experts, which allowed for identifying key vulnerabilities in various states and for preparing practical recommendations with respect to the national resilience enhancement.

Issues of ensuring resilience in different domains are studied by other well-known international organizations also.

Thus, the ***World Economic Forum*** (WEF) pays a big deal of attention to the national resilience studies and to the elaboration of recommendations for its development. In particular, the Annual Report "Global Risks 2013" suggested a methodology to assess national resilience to global risks (WEF, 2013). The Annual Report "Global Risks 2016" defined the ways to enhance national resilience through effective leadership and institutional values (WEF, 2016a). For instance, the document stressed the need to clearly identify roles and responsibilities to effectively respond to crises, ensure preparedness by means of exercises, trainings, and action planning; develop crisis leadership characteristics, in particular, the ability of leaders to make a quick and transparent decision, counteract corruption, maintain a high level of the public trust; create expert networks allowing for anticipating and analyzing risks and their impacts, which contributes to effective risk management; create a culture of the integrated risk management and multilateral partnerships.

The "Resilience Insights" report offered recommendations with respect to enhancement of resilience of the state and society to water supply crises caused by climate change, large-scale migrations and cyber-attacks (WEF, 2016b). Within the framework of certain studies for the World Economic Forum, experts also analyzed vulnerabilities of specific states to certain risks (in particular, Nepal, Latin America, Western Africa, Canada, and others) and developed recommendations with respect to enhancement of the respective types of specific resilience (WEF, 2015, 2020a; Guilbert, 2015, November 16; Faruqee & Pescatori, 2013).

Studies of the World Economic Forum pay a great deal of attention to issues of cyber-resilience. Thus, the report "Systems of Cyber Resilience: Secure and Trusted FinTech" examines the issue of the cyber-security and cyber-protection of financial systems (WEF, 2020b), and the guide "Cyber Resilience Playbook for Public-Private Collaboration" examines the architecture of public-private partnership in the aforementioned area (WEF, 2018).

Lately, World Economic Forum promulgated a number of reports concerning recovery after the COVID-19 and the search for ways to enhance the national resilience. The study "Principles of Strengthening Global Cooperation" states that today's recovery and enhancement of resilience to tomorrow's threats requires a global interaction with the involvement of many stakeholders. Also, according to WEF experts, it is important for the national resilience enhancement to promote peace and security, deepen public-private partnerships, prohibit all kinds of discrimination, prevent further stratification of the world, and restore the sustainable development (WEF, 2021a).

The document "Global Future Councils Nominations 2020–2021 Terms" envisages a number of studies in various areas of the national resilience enhancement, in particular, with respect to cyber-threats, border threats, as well as the formation of sustainable business models in various sectors, new approaches to the fragility and resilience of states, etc. (WEF, n.d.).

The report "Global Risks 2021" with consideration of the experience gained during the COVID-19 pandemic indicates that the lessons learned from this crisis gave an idea of not only how to prepare better for the next pandemic but, most of all, how to enhance the risk management processes, the respective capabilities, and communication culture. In view of this, WEF experts suggested four directions for strengthening resilience of states, businesses and the international community: 1) identify an analytical framework that would suggest a holistic and systems-based vision of the risks and their impacts; 2) invest in the largest-scale and detrimental risks ("risk champions") to encourage national

leadership and international cooperation; 3) improve communications concerning risks and combat misinformation; 4) develop new forms of public-private partnership with respect to risk preparedness (WEF, 2021b).

International organizations engaged in studies of the ensuring resilience in various domains also include the ***Organization of Security and Co-operation in Europe*** *[OSCE]***,** which raises issues of resilience of local communities to inflows of migrants, resilience of institutions to corruption, and disaster risk reduction, etc. (OSCE, 2017, 2020, n.d.).

In general, the results of the analysis of activities of the leading international organizations and states' alliances allow for affirming that all of them deal with certain issues of enhancing resilience of the state, society, communities, etc. The area of research, selection of the resilience objects, and directions of the respective practical efforts depend significantly on an international organization’s specialization, qualification, and experience of the involved experts. The key types of the international organizations’ activities with respect to the national resilience enhancement consist of examination of the effective practices, analysis, and development of recommendations for Member States and partners, or rendering experts’, organizational, financial, and other support to the states that need it.

Differences in conceptual approaches of the aforementioned international organizations and state alliances to ensuring national resilience which have been observed during the last years are provided in *Table 3.1*.

Table 3.1

International Organizations' and Alliances' Main Goals and Conceptual Approaches to Building National Resilience

International Organizations and Alliances	Resilience ensuring approach used before	Recent changes to resilience ensuring approaches	Main goals of ensuring resilience
NATO	Resilience as a component of collective defense and deterrence	Expand areas of civil-military interaction; greater attention paid to societal resilience	Adapt to uncertainty; timely identification and elimination of vulnerabilities; development of respective capabilities and interaction
EU	Resilience within the context of sustainable development and mostly in the external actions (support to developing, weak of conflict-affected states in building their resilience)	Implement wide approach to resilience; greater attention to enhancement of resilience of the EU and Member States; enhance the defense and security components of the EU policy as areas to increase the resilience	Providing: - ability of Member States and the whole Union to confront the full spectrum of threats without prejudice to common democratic values; - trust to institutions; - sustainable development; - good governance; - ability to reform

UN	Eradication of causes of vulnerabilities of states and their societies; adaptation to climate change; disaster risk reduction; ensuring conciliation and trust, etc.	Greater attention to security issues; expansion of spectrum of causes generating vulnerabilities in the society	Enhance states' crisis management, develop risk management systems, enhance civil protection and interaction between the government and population, enhance resilience of energy, water, food supply, transport systems, etc.
OECD	Enhancement of opportunities of individuals, communities and developing states to absorb risks and shocks they usually deal with, adaptation to their impact	Expansion of research areas and geography	Enhance risk assessment and organize the respective efforts on the basis of wide cooperation; identify vulnerabilities of states and their societies; support in development of national strategic and program documents with respect to the national resilience enhancement, etc.

Source: developed by the author

As analysis of the leading international organizations' and states alliances' documents and practices shows, revision of their conceptual approaches to the national resilience development takes place under influence of certain events that have a major impact on their main activities domains or on changes in the global security environment.

3.4. Foreign States' Experience in Providing National Resilience

3.4.1. Specifics of Selecting National Resilience Ensuring Model in Different States

The aforementioned international organizations and states alliances agree that the national resilience development is the nation's responsibility and states have to identify the related goals and priorities at their discretion. Now the states use various practices to ensure national resilience, which is explained by differences in their national interests, conditions, and peculiarities of their development.

Analysis of the specifics of shaping the state policy in national security and resilience, as well as of peculiarities of creation of such systems in countries like the United Kingdom, Denmark, Estonia, Israel, Canada, the Netherlands, New Zealand, Norway, Slovakia, USA, Hungary, Finland, Switzerland, Sweden, Japan, and others allowed for identifying a number of common features and differences in these processes (Reznikova, 2019c).

According to the results of the analysis of the world experience, different countries started with application of the national resilience ensuring mechanisms in the priority areas identified by them, where the risks were the highest and of the largest scale for the state and society. Mostly, the states chose such priorities as counteraction to terrorism, protection of critical infrastructure, cyber-security, natural and man-made disaster response, etc. The main goals of the state policy in national security and resilience were the following: ensuring a high level of preparedness for and effective response to key threats by all actors, reduction of threats` impact, and speeding up the pace of recovery after crises. Different states implemented universal and special mechanisms to ensure national resilience through the adoption of the respective regulatory acts, programs, action plans, manuals, etc. At the same, time while the national resilience

systems were being formed in these countries, they had certain differences related to diverse natures of the key threats for state and peculiarities of selection of the priority mechanisms and means with consideration of their effectiveness under specific circumstances, as well as of properties of the national mentality, historical, cultural, socio-political, and other features.

The main goals and objectives with respect to ensuring national resilience in the examined countries were identified in their strategic documents. In particular, the sets of objectives in different areas of ensuring national resilience were defined in the national security strategies of the United Kingdom starting from 2008. Thus, one of the main goals of the National Security Strategy (2010) was determined as strengthening the UK`s security and resilience, which included protection of the population, economy, infrastructure, territory, and the way of life against current and potential risks. At this, the ensuring of the state`s resilience was viewed in the context of increase of its preparedness for all kinds of threats, the ability to recover after crises, and to continue vital services (UK Government, 2010). National Security Strategy and Strategic Defense and Security Review (2015) defined as main goals of the internal policy defense, resilience and partnership. Also, the document identified the priorities to ensure national resilience to different types of threats and crises in various domains (UK Government, 2015).

National Security Strategy of Japan (2013) tackled strengthening resilience in the field of national security, in particular, through the development of diplomatic, military, economic and technological capabilities which contribute to peace and stability in the region and in the world, as well as the resilience to natural disasters (Office of the Prime Minister of Japan, 2013). According to official documents of the Cabinet Secretariat of Japan, the main principles to build up the national resilience in this country were defined as follows: prevention of human losses in any manner; providing continuous performance of important functions to maintain the public governance, as well

as social and economic systems; minimization of losses related to damages of property, structures, etc.; achievement of quick recovery and reconstruction after crises (National Resilience Promotion Office of the Cabinet Secretariat of Japan, n.d.).

In the USA, the comprehensive approach to national resilience was implemented only in the National Security Strategy (2017) (President of the United States of America, 2017). The strategies of the previous years, as well as other program documents, in particular, The 2014 Quadrennial Homeland Security Review, identified just certain objectives in the respective domain (US Department of Homeland Security, 2014).

Until recently, the strategic documents of many other countries also identified mostly selected activities to strengthen resilience of the state and society to certain threats. In particular, dramatic events that occurred in the USA on September 11, 2001, induced a number of countries to look for the ways to increase resilience of the state and society to the terrorist threat. Respective objectives were defined in the Counter-Terrorism strategies of Australia (2015) and Canada (2013), as well as in the US National Strategy for Homeland Security (2007) (Council of Australian Governments, 2015; Government of Canada, 2013; US Homeland Security Council, 2007). Counteraction to terrorism has always been one of the central ideas in the strategic and program documents of Israel (Belfer Center, 2016; Eisenkot & Siboni, 2019).

Countries that have suffered periodically from destructive impacts of natural disasters (earthquakes, floods, droughts, typhoons, etc.) and climate change started implementing measures aimed at enhancement of their resilience to these threats. In particular, appropriate plans were developed in Australia, Denmark, Canada, the Netherlands, New Zealand, Norway, the USA, Finland, Czechia, Switzerland, and Japan. Also, a number of documents were developed and implemented with respect to enhancement of the resilience in specific domains (economic, social, critical infrastructure protection, etc.) in such

countries as Estonia, Israel, Island, Spain, Canada, Poland, Portugal, USA, Turkey, Hungary, France, Czech Republic and Switzerland (OECD, n.d.a).

In view of Russia's hybrid aggression against Ukraine some countries (in particular, Slovakia and Finland), the EU, and international organizations started developing and implementing their strategic and program documents with respect to counteraction to hybrid threats (European Commission, 2016c; Office of the Prime Minister of Finland, 2017; National Security Authority of the Slovak Republic, 2018).

United Kingdom implemented comprehensive approach to national resilience, which included, first of all, ensuring preparedness to respond to various hazards (all-hazards approach). This approach, in addition to the National Security Strategy, was implemented in a number of state documents, among which Sector resilience plans, the Strategic National Framework on Community Resilience, The Resilience Capabilities Programme, and others should be noted (UK Cabinet Office, 2011, 2018a, 2019).

As pointed out above, peculiarities of selection by the states of their model to ensure national resilience were often related to the nature of the key threats to their national security. Analysis of strategic and program documents of various states allowed for finding out that the priority threats, in response to which the national resilience ensuring systems were initially built up, were defined as follows: terrorism in Israel, terrorism and natural disasters (typhoons and floods) in the USA, natural disasters (earthquakes, floods, typhoons, and tsunamis), emergencies and terrorism in the United Kingdom, external influences aimed at society destabilization (with the emphasis on informational and cyber domains) in Estonia. The aforementioned states' strategic and program documents that were adopted during previous years (starting from the past century and until 2014) and speeches of their leaders mentioned mostly these specific threats (Belfer Center, 2016; Eisenkot & Siboni, 2019; President of the United States of America, 2017; Office of the Prime Minister of Japan,

2013; Republic of Estonia Ministry of Defence, 2017; UK Government, 2010, 2015; US Department of Homeland Security, 2014).

As a rule, destructive impacts of threats (including terrorism and natural disasters) mostly affect the population. The examined practices with respect to ensuring national resilience used by various countries demonstrate that a significant part of the respective activities and mechanisms were aimed at enhancement of effectiveness of the population protection against key threats, as well as at strengthening societal and individual resilience to such threats.

Also, the key threats defined by many countries (first of all, terrorism and natural disasters) can destroy or cause significant damage to the critical infrastructure, which, in turn, can lead to cessation of providing critical services to the population (supply of energy, food, and water, medical care, transport, etc.). In view of this, many countries selected as a specific area of ensuring national resilience the establishment of the system of critical infrastructure protection and security. This comprehensive institutional mechanism focuses on unification of efforts of authorized stated bodies, private businesses, citizens, and civil society organizations, as well as clear distribution of their responsibilities. Critical infrastructure protection systems were established, in particular, in the USA, Canada, Sweden, and other countries.

The United Kingdom organized the national resilience ensuring cooperation not only at the inter-agency level but also in the format of a local resilience forum, where representatives of both authorized ministries and agencies and local governments and societies participate. It should be added that in this country, significant responsibilities and powers in the national security and resilience domain are entrusted to the regional and local authorities and communities. According to the UK Cabinet Office (2011), most of the measures ensuring community resilience do not need significant financial resources but require the right organization of the respective processes.

With respect to organization of links between central and local authorities and communities, the US experience certainly deserves mentioning. One of the main functions of the Federal Emergency Management Agency [FEMA], which is a part of the US Homeland Security Department, is to ensure national resilience. Within this agency, a special structural unit was created. This unit concentrates its efforts on forming a culture of preparedness for emergencies (first of all, natural and man-made ones). The mechanisms suggested to achieve this goal are emergency insurance and planning, awareness campaigns for the public, exercises, preparation of the methodological recommendations, and other documents (FEMA, n.d.b). The state renders the required methodological and organizational assistance to the local governments and citizens which then decide on their resilience enhancing activities at their own discretion. To implement such activities, different actors are eligible for target grants.

Also, the USA pays a big deal of attention to the development of various formats of inter-agency cooperation on the issues of counteraction to various threats; within such formats, information is continuously exchanged among the public authorities, risks are analyzed, best threat-overcoming practices are shared, recommendations on acting during crises are developed and priority objectives to enhance resilience of the state, society and communities are defined. According to the well-known conclusions of US experts, one of the essential gaps in the US anti-terrorist security system that made the large-scale terrorist attacks on September 11, 2001, possible was the lack of proper communications between different agencies and special services. In view of this, another mechanism to ensure US national resilience was strengthening the US Intelligence Community, which allowed for improving coordination of intelligence and counterintelligence authorities and the exchange of information between them and also fostered capability development with respect to threats anticipation and increase of preparedness to respond in a timely and adequate manner.

The US, Israel and the UK view as an important element to fight crime and especially terrorism, an active involvement of the population in assistance to law enforcement in the respective sphere (for instance, reporting suspicious activity, participation in organization and implementation of awareness campaigns, exercises, etc.). Thus, the USA implemented a number of programs (The Fairness Award, "If you see something, say something", The Neighborhood Policing Initiative, etc.) aimed at making the public interested in reporting to law enforcement bodies any suspicious activity having signs of terrorism. Other examples of effective interaction between the state and society to counter a wide spectrum of internal threats are activities of non-governmental volunteer police assisting organizations (in particular, Crime Stoppers in the USA, Ha-Mishmar Ha-ʿEzraḥi in Israel, and local police support forces in the UK) and volunteer firefighters, implementation of the mass media cooperation programs, etc. (Reznikova, 2018c).

A separate vector of the state policy in national security and resilience in the countries studied is the enhancement of public awareness concerning current and prospective threats and mechanisms to counteract them. The establishment of publicly available national risk registers or profiles in the United Kingdom, the Netherlands, and New Zealand is an example of such states' activities. They contain the necessary concise and understandable information on the nature of the most likely threats, action plan of the population and authorized state bodies in the case of an emergency or crisis, contact phone numbers and other important recommendations. Also, a number of states have widely spread practice of active involvement of the public associations in the implementation, jointly with the law enforcement bodies, of awareness campaigns for the population with respect to the nature and manifestations of the modern terrorist threat, development of indicators of possible terrorist activity, preparation of the information materials, organization of case studies, drafting of regulatory acts on the fight against terrorism and other illegal activities, implementation of anti-

terrorist trainings and exercises for the public, etc. Besides, the states pay proper attention to the establishment of reliable bilateral communication channels with the public.

So, implementation of the aforementioned activities contributes to the development of the proper security culture of the public, increases the level of the society`s self-organization and trust in the government, decreases anxiety, and as a result - reduces vulnerabilities to direct and indirect impacts of threats and crises (physical, psychological, behavioral, social, political and others).

In the modern world, there are widely spread destructive informational and psychological impacts on the population and some of its layers as an element of hybrid threats. In view of this, the states intensify their activities in respective areas of enhancing national resilience. In particular, in Israel and the USA, a big deal of attention is paid to psychological aspects in development of society's resilience to the terrorist threat and in Estonia mechanisms of societal resilience to negative informational and communication impacts are intensively developed.

An important point is that all of the countries under examination believe that economic destabilization is one of the major threats to national security. Main strategic and program documents of these states concerning national security and resilience development always include activities aimed at enhancement of the national economy`s resilience and ensuring continuity of business processes under crisis circumstances.

To summarize the above, one can affirm that the development of national resilience ensuring mechanisms in different countries has its specifics. With consideration of the fact that this process is quite dynamic, the *priority areas of ensuring national resilience formulated by the states at the beginning have formed certain peculiarities of the respective system but have never impeded later further development and expansion of such system.* The states under examination have been developing their national resilience ensuring systems

simultaneously with development of their national security ensuring systems and effective capabilities.

Now many states (in particular, Australia, the United Kingdom, Estonia, Canada, Latvia, the Netherlands, New Zealand, the USA, and others) updated their strategic and program documents on national resilience. According to Fjäder (2014), most of the national security strategies examined by him, implement a new paradigm, which is based on embracing all kinds of threats to the whole society.

In particular, in the Netherlands there are clearly visible principles of ensuring national resilience in their modern approach to counteracting threats to the state. Main goals and measures of the respective state policy contain the implementation of the standard operating procedures (including with regards to definition of national interests, identification of threats, enhancement of national resilience); strengthening information component (including timely identification and correct interpretation of threats jointly with partners both in the country and abroad); increase of risks and threats awareness (of local managers, diplomats, critical infrastructure companies management, public, etc.); development of knowledge concerning risks, threats and counteractions; application of a wide spectrum of defense measures (including diplomatic tools); strengthening connections between economy and security (including analysis of foreign investments regarding their impact over national security, protection of critically important technologies, etc.); enhancing digitalization; development international cooperation (The Netherlands National Coordinator for Security and Counterterrorism, 2019a).

The most widespread universal mechanisms to ensure national resilience in different states are the following:

- comprehensive risk and threat assessment, anticipation and simulation of crises, and identification of vulnerabilities;

- ensuring preparedness and planning of concerted measures on the basis of whole-of-society cooperation;
- crisis management to ensure regulation and coordination of measures at all stages of the national resilience ensuring cycle, partnership among the participants, accountability, economic efficiency;
- establishment of regional and local security capabilities on the basis of subsidiarity and institutional multilateral interaction formats.

The analysis of strategic and program documents and practices of different states allows for identification of changes that have taken place in the national resilience ensuring model: from concentration on priority domains and areas to the comprehensive approach to ensuring preparedness to respond to various threats on the basis of whole-of-society cooperation. Major shifts in formulations of national policies in national security and resilience have been observed in different states precisely after 2014.

Nowadays, states have different ways to establish their own priorities in national resilience. Some concentrate on strengthening threat and hazard anticipation capabilities in order to prevent and minimize the impact, others aim their main efforts at enhancement of preparedness to respond to emergencies and threats of any origin with consideration of the fact that most of them are difficult to predict and to identify at an early stage. This specifically applies to hybrid threats. Sometimes, more attention is paid to the aspects of generations of the required reserves and resources for prompt recovery after an emergency or crisis.

3.4.2. Peculiarities of National Resilience Ensuring System in Different Countries

Based on the national resilience ensuring model selected with consideration of the national interests, the states build appropriate legal and institutional support systems. Within these processes, it is extremely important

to ensure effective interaction of governmental and non-governmental actors along the key lines of ensuring national resilience at different stages (before, during and after the crisis), and to coordinate such activities at different levels: strategic, operational and territorial.

The world experience demonstrates that effective national ensuring systems are sufficiently centralized, and decisions on threat response are made at the lowest level possible (local). At the same time, respective activities are coordinated, common and understandable for all stakeholders rules, standards and procedures of concerted actions at different stages of the resilience ensuring cycles that are defined at the highest reasonable level determined by each state individually.

Analysis of the world experience conducted with respect to coordination of activities to ensure national resilience *at the strategic level* gives reasons to affirm that in the states with a parliamentary system, such function is mostly performed by the government (Reznikova & Siomin, 2020). As usually, an authorized unit (or units) within the government's office (prime minister's office) is empowered to draft regulatory acts on key issues of ensuring national resilience, establish communications among the stakeholders and relations with foreign partners, etc. The establishment of permanent interagency working groups and networks on various national resilience issues is a common global practice. They include representatives of public authorities, research institutions, and a civil society.

In the United Kingdom, the Netherlands, Norway, Switzerland, Denmark, Estonia, and New Zealand, government coordinates the activities aimed to ensure national resilience including crisis management and preparation of the recommendations and guidelines for other stakeholders. Its secretariat (or office) includes specialized units dealing with different issues of building national resilience and, as a rule, they are closely linked with the public authorities

(institutions), which are responsible for the national security and crisis management issues, and empowered to support the following processes:

- drafting regulatory acts, guidelines and recommendations for various target groups (public institutions, communities, population, businesses, etc.);
- coordination of the overarching planning of activities to ensure national security and resilience at all stages (before, during and after the crisis) and to develop the required capabilities;
- development of public-private partnership;
- organization of purposeful trainings and exercises to share the required knowledge and skills;
- creation of resilient inter-agency communications, as well as networks with participation of research institutions and civil society in the matters of ensuring resilience;
- organization of international cooperation in the respective sphere.

For instance, in the United Kingdom the National Security Adviser [NSA], who is the head of the National Security Secretariat [NSS], coordinates the governmental policy with respect to the national resilience development. An important role belongs to the Civil Contingencies Secretariat [CCS] of the Cabinet Office, which is responsible for the coordination of activities of the Cabinet Office departments and other governmental and non-governmental organizations in the matters of ensuring national resilience (UK Parliament, 2002). In particular, CCS is responsible for interaction with the Resilience and Emergencies Division in the Ministry for Housing, Communities and Local Government (is now called Department for Levelling Up, Housing and Communities), supports activities of the Civil Contingencies Committee [CCC] and interaction with representatives of businesses on the matters of providing civil preparedness, etc. Also, its powers include development and implementation of the Resilience Capabilities Programme, implementation of

the national risk assessment, the keeping of National Risk Register, forming and implementation of the state policy in national infrastructure security and resilience and corporate resilience policy in the private sector, etc. (UK Cabinet Office, 2018b).

In general, the UK Government has always been paying a great deal of attention to the matters of national resilience. Usually, the priorities of the state policy in this area have been defined as follows: to augment capabilities to prevent and counteract threats, minimize the impact and ensure quick recovery, enhance the critical infrastructure resilience to the destructive impact of conventional and non-conventional threats, provide continuous functioning of the Central Government and of its ability to solve complicated tasks of threat prevention and minimization of vulnerabilities, and spread information on current and potential crises, etc.

In the Netherlands, activities to develop national resilience at the strategic level are also coordinated by the government. The main authorized body is the National Security Steering Committee (Dutch: Stuurgroep Nationale Veiligheid)[10], established due to the Order of the Minister of Interior of 18 February 2010, No 85920. This ministry is responsible for the state policy coordination in the field of national security and crisis management at the national level.

The aforementioned Committee is a national platform for enhancement of national resilience because its composition includes heads of all public ministries and agencies, as well as representatives of businesses and civil society who are included as advisors[11]. The Committee ensures concerted character of the national security policy and crisis management at the regional and national levels, as well as in the sphere of foreign relations and development. Besides, the Committee takes part in development and implementation of the state policy,

[10] *Instellingsbesluit Stuurgroep Nationale Veiligheid.* https://wetten.overheid.nl/BWBR0027277/2010-02-23

[11] UN Office for Disaster Risk Reduction. *Netherlands, the National Platform.* Retrieved from: https://www.preventionweb.net/english/hyogo/national/list/v.php?id=122

advises the Government and Parliament on the emergency risks and measures of their mitigation, development of the respective capabilities and concerted actions.

The Committee Head is the State Director for Security of the Ministry of Interior. The Committee Secretariat functions within the Ministry of Interior. In order to ensure the inter-agency coordination and interaction, the Committee has an inter-agency working group for national security (*Dutch:* Interagency Werkgroep Voor Nationale Veiligheid), which includes representatives of various ministries and agencies.

An important role in coordination at various levels of ensuring national security belongs to the National Coordinator for Security and Counterterrorism (*Dutch:* Nationaal Coördinator Terrorismebestrijding en Veiligheid, NCTV)[12] who operates within the Ministry of Justice and Security (*Dutch:* Ministerie van Justitie en Veiligheid). In particular, the National Coordinator ensures exchange of information among all actors in the national security field, is responsible for reliable functioning of threat prevention and response mechanisms, and monitors correspondence of the national security policy and crisis management to the rules of the national legislation, treaties on international cooperation and the EU legislation.

In Norway, the Cabinet of Ministers has the supreme responsibility (including political one) for management and control in the sphere of ensuring preparedness and threat and disaster response (as the basis of national resilience) (Norwegian Ministry of Defence, Norwegian Ministry of Justice and Public Security, 2018). By the decision of the Prime Minister of Norway, the respective work can be conducted through the Government`s Security Committee, where the key participants are the Prime Minister, Minister of Foreign Affairs, Minister

[12] *De Nationaal Coördinator Terrorismebestrijding en Veiligheid.* https://www.nctv.nl/organisatie

of Justice, Minister of Defence and Minister of Finance while their work is supported by the Prime Minister's Office.

The authority in charge of administrative coordination at the top ministerial level is the Emergency Council which includes five permanent members: the Secretary to the Government at the Prime Minister's Office, the Secretary General at the Ministry of Foreign Affairs, and the Permanent Undersecretaries of the Ministry of Justice and Public Security, the Ministry of Health and Care Services and the Ministry of Defense; if necessary, representatives of other institutions can be involved. The functions of the Council for Crisis Situations are security environment assessments; coordination in various areas, as well as sharing information with the public, media, etc.; expedited clarification of powers and budget in complicated situations. The Council meetings are mostly chaired by representatives of the Ministry of Justice and Public Security, which plays a leading role in crisis management.

It should be noted that Norway implemented the comprehensive approach to national security and resilience according to the total defense principle, which overarches the matters of defense, civil protection and crisis management. This, among others, provides clear distribution of responsibilities and cooperative interaction in peacetime and wartime between the Ministry of Justice and Public Security and the Ministry of Defense of Norway. All Ministries and Agencies, which are responsible on a daily basis for an area, are also responsible for prevention, emergency preparedness, and the implementation of necessary measures in emergencies and disasters. At this, the organization that comes into operation during crises should be as similar as possible to the organization that operates daily. The National Total Defence Forum is a permanent platform for cooperation of the heads of key civilian and military institutions which discuss general issues related to the defense, civil-military interaction, civil protection, and preparedness for crises (Norwegian Ministry of Defence, Norwegian Ministry of Justice and Public Security, 2018).

In Sweden, state policy in crisis management (as the key mechanism to ensure national resilience) at all national levels is coordinated by Swedish Civil Contingencies Agency (*Swedish:* Myndigheten för samhällsskydd och beredskap, MSB) (Swedish Civil Contingencies Agency, 2019). The main responsibility for planning and implementation of risk reduction and crisis management activities is entrusted to the local municipalities. Higher level (regional and national) authorized bodies (in particular, the aforementioned agency) are engaged only when an emergency or crisis cannot be coped with at the local level.

The Swedish Civil Contingencies Agency is a governmental organization empowered to provide emergency preparedness, crisis management, civil protection, cyber-security, planning and implementation of exercises and training, conducting specific operations in tight cooperation with ministries, municipalities, and the private sector. The Agency is headed by a Director General appointed by the Government. This Agency's structure includes the following divisions: Emergency and Civil Defense Preparedness Department; Civil Protection and Accident Prevention Department; Directorate of Operations; Directorate for Cyber-Security and Communications Security, and others (Swedish Civil Contingencies Agency, 2019).

In New Zealand, the Government has the main responsibility for the national security and resilience. The Cabinet National Security Committee is responsible, first of all, for consideration of strategic, political and legislative matters concerning national security and resilience, intelligence, defense (except for defense procurement), and large-scale threats. The Committee coordinates and directs national responses to major crises or circumstances affecting national security. It is chaired by the Prime Minister and includes senior ministers including ministers of finances, defense, economic development, healthcare, communications, and foreign affairs, as well as, prosecutor general, heads of police, special services, customs office, immigration office, and other officials,

when required (New Zealand Department of the Prime Minister and Cabinet, 2016).

In general, matters of organization of national resilience ensuring activities are regulated in the studied states by ramified legislation. In addition to special laws defining the powers and responsibilities of different public authorities and procedures of their interaction in varied conditions (in particular, in peacetime and wartime) there are various guidelines and recommendations for different target audiences (ministries and agencies, local communities, training institutions, specific groups of population, etc.). Such documents describe the ways to prepare for a disaster or crisis, the reserves that need to be generated, the way to plan anti-crisis activities, how to conduct exercises and trainings, what to do during and after crisis, etc.

The analysis of world experience of ensuring national resilience demonstrates that many states implement the principle of subsidiarity, according to which an effective cooperation to build up national resilience and establish the required institutional mechanisms is organized not only at the national level, but, first of all, at the *regional* and *local levels*, because they are the levels where the effective primary response to threats and crises is expected to be implemented (Reznikova et al., 2021).

In this context, the experiences of the Netherlands and the United Kingdom deserve attention, where comprehensive multi-level national resilience ensuring systems operate. These states created effective formats of inter-agency interaction and ensuring regional resilience and resilience of territorial communities: Security Regions (in the Netherlands) and Local Resilience Forum (in the United Kingdom). To organize such permanent comprehensive mechanisms of inter-agency cooperation it is necessary to define clearly their missions, main goals and objectives, peculiarities of legislative, institutional and methodological support of their activities, distribution of powers between the state, regions and local communities, etc.

The Netherlands has an effective mechanism of interaction between the central and local authorities, non-governmental organizations, and businesses on issues of ensuring national resilience, which is implemented, in particular, through the Security Regions institution.

Security Region (Dutch: Veiligheidsregio's) is a special format of the public administration in the sphere of regions' security and resilience, which allows for amalgamation of capabilities of various local communities, establishment of a common governance and legal regulation authority in order to provide an effective coordination of activities and enhancement of interaction. The main regulatory document concerning the relations in this sphere is the Law of the Kingdom of the Netherlands "On Security Regions" (*Dutch:* Wet veiligheidsregio's) as of 11 February 2010 (Wet veiligheidsregio's, 2010).

In order to integrate local communities' capabilities to effectively counteract emergencies and crises, the Netherlands generated, within 12 provinces, a network consisting of 25 Security Regions. One to four Security Regions operate in a decentralized manner in each province. Each Security Region includes from 6 to 24 municipalities. The relevant cooperation of local communities is organized on the basis of agreements on municipal cooperation and collective responsibility. Local communities (municipalities) are territorially joined into Security Regions with consideration of their specific category of risks and threats and peculiarities of the security situation in a certain part of the state, as well as on its borders with neighboring countries Germany and Belgium[13].

The key function of the Security Regions is an effective response of local communities to emergencies at their level. This is achieved through implementation of a single security and resilience ensuring system, integration of resources, enhancement of capabilities and their rational use, ensuring

[13] *Over de veiligheidsregio. Veiligheidsregio Gooi en Vechtstreek.* https://www.vrgooienvechtstreek.nl/onze-organisatie/de-veiligheidsregio/

preparedness to respond to different threats and crises. The point of major importance is to arrange an effective interaction of municipalities and local communities, quick response services (firefighting, rescue, medical, environmental, epidemiologic, anti-flood, police, ambulance, etc.), crisis management authorities, regional logistic and informational support, private enterprises and volunteers' organizations, territorial units of the public authorities (first of all, security forces: Army and Navy, Coast Guard, special services, water resources control and security authorities), critical infrastructure enterprises, etc.

The main tasks of the Security Regions are:

- analyzing and assessing risks and capabilities to counteract emergencies;
- planning activities in the sphere of security and resilience of amalgamated local communities;
- consulting Security Regions' actors with respect to emergency risks;
- enhancement of resilience of local communities and critical infrastructure to significant risks, increase their preparedness for crises, as well as implement an appropriate system to prepare the population and quick response services to act in emergencies and crises;
- coordination and support of the emergency quick response services, units of emergency medical aid, technical and operational support, delivery of the required equipment, etc.;
- providing emergency preventive and response measures, ensuring development of protective engineering infrastructure in the Security Region;
- ensuring appropriate information sharing among Security Region actors (as well as with neighboring regions, Ministry of Security and Justice, Army, etc.), development of security information centers, continuous operation of cyber-systems, establishment of resilient communications with the population;

- development of civil defense system in Security Region within civil-military cooperation network, as well as volunteers' activities;
- development of trans-border cooperation (if the Security Region is located near the state border) with neighboring territorial communities of Belgium and Germany with respect to joint response to threats, emergencies and crisis situations (Wet veiligheidsregio's, 2010).

Within the Security Regions, municipalities and other authorities of local communities (including cities, city districts, etc.) functioning in a certain administrative territory in a province of the Netherlands unite their efforts to develop their resilience. Collegiums of Mayors of different municipalities, municipal councils, and councils of local communities in the cities are established for solving the vital problems in this field.

General management of the Security Regions is conducted by the councils composed of Mayors of municipalities forming the Region. The Security Region Council Heads are appointed by the Royal Decrees by proposals of the Mayor's collegiums of the Regions after an interview conducted by the authorized Royal Commissionaire. Council Head's activities are supported by the Head's Staff which, includes, in particular, directors of departments responsible for fire, environmental, man-made disaster, epidemiologic and public safety and security, rescue and medical aid, crisis management, the fight against cyber-threats, flood control, etc. Within the aforementioned branches, different branch working groups are established and function; they are headed by directors of the respective profile departments. Chief Province Prosecutor (or his/her deputy), head of water resource department, and authorized Royal Commissionaire who is a liaison between the Security Region and the Government are always invited to take part in the meetings of Security Region Councils.

Heads of Security Region Councils appoint municipality activities coordinators. In crises, additional Region operational managers are appointed

who are in charge of the general management of the Security Region`s quick response services.

Security Regions have a standing Political Group (composed of Municipality Heads and Prosecutor) responsible for crisis management and security policy making. In the case of an emergency, the Region Operations Group (composed of Municipality quick response service directors) mitigate the impact of disasters. Such groups are headed by Region operational managers.

Also, there are Region Inspectorates, the key objectives of which are: to assess quality of crisis management and policy in security and resilience of the Security Regions; inspect critical infrastructure facilities to check compliance with safety requirements and the level of competence of authorized officials; to check preparedness of Security Regions and their actors to respond to emergencies; to conduct investigations and audits.

The system of collective advisory bodies and working groups at the municipality level in the Netherlands are built according to a similar principle. A single center for operational control, which operates under the office of the board of a Security Region, coordinates activities of Municipalities` response services. Prevention of and response to emergencies measures are performed with participation of local private enterprises and civil society organizations. Steering authorities of Security Regions conclude with them annual cooperation agreements including social responsibility obligations.

In order to provide operational monitoring of security environment devolvement, the Netherlands established a network of the monitoring and dispatching systems at national, regional and municipal levels (so called control rooms). To provide adequate informational support, Security Region information centers were established, and to ensure effective interaction of Security Regions, a single information and communication system was founded. The state has developed systems to communicate with the population and to give alert messages. Each Security Region has its site on the Internet.

An important area of the Netherlands Security Region activities is security and resilience planning within amalgamated local communities. This process includes a consistent drafting of a number of publicly available documents such as Regional Risk Profile (*Dutch:* Regionaal Risicoprofiel), Regional Security Policy Implementation Plan, Crisis Response Plan, as well as Natural Disaster Response Plan, which are developed for private partners involved in emergency response activities in the Security Region. Based on the aforementioned documents, Municipalities identify priorities, goals, and objectives and plan their activities in the field of local communities` security and resilience enhancement.

At the national level, public governance and control over the Security Regions are implemented by the Ministry of Justice and Security of the Netherlands (*Dutch:* Ministerie van Justitie en Veiligheid)[14], which operates under the supervision of the National Coordinator for Counterterrorism and Security (*Dutch:* Nationaal Coördinator Terrorismebestrijding en Veiligheid, NCTV) within the aforementioned Ministry[15].

The Security Regions Network is the key link within the national crisis management system, which ties together formation and implementation of the national security and resilience policy of the Netherlands at central and local levels. It is stipulated that the state government never interfere in the shaping and implementation of respective policy by Security Regions. At the same time, Security Regions are expected to take into consideration national legislation and commonly adopted approachs to development of such policy in the country, specificly for their territories risks and threats, capabilities, as well as goals and objectives of the state, the implementation of which are mandatory at local level in the Netherlands in accordance with the National Risk Profile [NRP] (The Netherlands National Network of Safety and Security Analysts, 2016). Also, the

[14] *Ministry of Justice and Security*. https://www.government.nl/ministries/ministry-of-justice-and-security
[15] *The National Coordinator for Security and Counterterrorism*. https://english.nctv.nl/organisation

governmental authorities never interfere with activities of Security Regions in the case of local emergencies. Security Regions are supposed to respond to emergencies, crises, or other threats on their own but can expect reimbursement of expenses by the state. If emergencies or crisis's evolve to a national scale level, governmental authorities (in particular, the Ministry of Justice and Security and the National Coordinator for Counterterrorism and Security) have the right to intervene in the localization of local emergencies and mitigate their impact.

In the **United Kingdom,** within England, Wales, Scotland, the Northern Ireland, there is a system of ensuring local communities' resilience to emergencies on the basis of partnership interaction. The key institution here is the *Local Resilience Forum* [LRF][16]

The UK system of ensuring resilience of local communities is founded on principles of collective responsibility, subsidiarity, integration, continuity, purposefulness, multi-level interaction, and coordination, as well as cooperation with civil society and businesses. It is adaptable to changes in the security environment due to the developed direct and inverse organizational, managerial, and information links between local, regional and national authorities. The system ensures concert and balance of interests and goals of all levels of government and local communities of the United Kingdom through integrated crisis management, division of powers and responsibilities, planning for crisis preparedness, capacity building, and their rational use, flexible response to large-scale emergencies in the United Kingdom, defining the legal order and framework for the application of special powers in an emergency. The functioning of the Local Resilience Forum is based on the following main processes: anticipation and assessment of risks; emergency prevention;

[16] *Local resilience forums: contact details.* https://www.gov.uk/guidance/local-resilience-forums-contact-details

providing preparedness; response to an emergency; recovery from the emergency (UK Cabinet Office, 2013).

Operations control and decision-making with respect to local emergency response and recovery are implemented at the local level in the United Kingdom. Emergency services (police, firefighters, paramedics, etc.), health care services, local and public authorities are supposed to have emergency plans. These plans should involve other stakeholders (for instance, utility operators). The level of involvement of non-governmental actors, civil society, and the private sector depends on the arrangements between them and local authorities. Volunteers formally participate in preparedness, response, assistance and recovery activities. The involvement of the Armed forces occurs only as a last resort, when necessary.

Civil Contingencies Act (UK Parliament, 2004) is a basic legislative act to ensure national resilience in the United Kingdom. Its provisions are evolved through a number of national regulatory acts of respective profiles. In particular, Strategic National Framework on Community Resilience determines capabilities of communities and individuals to prepare for various emergencies, gives examples of how communities and citizens can help themselves with their own resources and through interaction with special services before, during and after crisis (UK Cabinet Office, 2011). This document is not binding but explains the ways to establish joint capabilities of different actors to counter threats of different nature and suggests a kind of “road map”. Another purpose of this document is to enhance dialogue between governmental entities, special emergency services, authorized stated bodies, local governments, private sector, research institutions, civil society organizations, local communities, and resilience building target groups.

The main function of the Local Resilience Forum is to ensure effective coordination of inter-agency activities and integration of assets, means, and capabilities (managerial, rescue, medical, police, volunteers, municipal, reserve,

and others) of local communities and central authorities (armed forces, coastal guards, national transport police, telecommunications agencies, and others), which operate on their territories, in order to provide preparedness and response to emergencies and crises of natural, man-made, biologic, social and of other natures at the local level. Important tasks of the forum are coordination of risk assessment processes at the local community level, planning of capacity development activities (institutional, material, engineering, etc.), prevention and response to emergencies, and recovery. Particular attention is paid to comprehensive preparation of local communities to respond to possible crises and threats of various origins based on the whole-of-society approach.

The territorial area of responsibility of the local resilience forum is mostly limited by the areas of responsibility of local police services (region, several regions, county), which can cover over ten local communities and where the ramified quick response services network (firefighting and rescue teams, emergency aid stations, police forces, utility repair services, etc.) operate. It is assumed that local communities in big cities (at the level of districts and neighborhoods) can also form local resilience forums.

The subsidiarity principle constituting the basis of the UK local resilience forums network provides for the transfer of powers and responsibilities for crisis management to local authorities within the defined territories, subject to maximum coordination of their activities by senior administrations and central governments in compliance with national law.

At the level of countries and regions of the United Kingdom, other permanent formats of inter-agency cooperation in the field of resilience-building are established. They provide coordination between local resilience forums and higher-level authorities. In particular, there are Wales Resilience Forum [WRF][17], Regional Resilience Partnerships [RRP] in Scotland[18], Civil

[17] *Wales Resilience.* https://gov.wales/wales-resilience/what-we-do
[18] *Preparing Scotland: Philosophy, Principles, Structure and Regulatory Duties.* https://ready.scot/

Contingencies Group in Northern Ireland [CCG(NI)][19], and London Resilience Forum [LRF][20]. They define strategic approaches to local communities' resilience in the countries/regions, coordinate activities at district and local levels, as well as maintain linkages with other countries/regions and central ministries of the UK in the respective domain. Local resilience forums act independently of regional resilience forums and recognize only their strategic leadership in coordination of joint efforts within the country/region. Activities of regional resilience forums are supported by various committees, collegiums, working groups, and sub-groups. Emergency coordinators that provide interaction with the central government operate within devolved governments. Informational interaction between local resilience forums, higher-level coordination entities, and other partners is supported through a single informational network National Resilience Extranet[21].

Important tasks of local resilience forums include periodic risk and threat assessments at the local level, the generation of threat preparedness plans, containment, and minimization of the impact of emergencies and threats of any nature.

The functioning of local resilience forums envisages regular inter-agency meetings with participation of representatives of local governments, civil society, mass media, etc. The forums are not legal entities but ensure collective responsibility of all participants for planning and preparation for emergencies. Decisions of such meetings are not binding for their members but have the purpose to regulate urgent issues of organizational, resource, informational and other nature.

[19] *The Executive Office. Civil Contingencies.* https://www.executiveoffice-ni.gov.uk/articles/civil-contingencies
[20] *London Resilience Forum.* https://www.london.gov.uk/what-we-do/fire-and-resilience/london-resilience-forum
[21] *National Resilience Extranet – Common Operating Picture.* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/79249/National_Resil ience_20Extranet_20Common_20Operating_20Picture_20v1_1_20slides.pdf

The UK legislation divides authorities and organizations responsible for emergency planning and response as well as those involved in the local resilience forums into two categories:

Category 1: representatives of local authorities, emergency services (police, firefighters and rescuers), health care and emergency medical services, maritime and coastal emergency service, environmental agencies, etc. According to the law, members of this category have a duty to take part in the work of these forums;

Category 2: representatives of utilities (energy and water supply services, etc.), transport companies, airport operators, representatives of civil society, volunteers' organizations, etc. Members of this category may participate in local resilience forums and, if required due to the situation, are obliged to provide support to participants in category 1 (UK Cabinet Office, 2013; UK Parliament, 2004).

The structure of local resilience forums may vary region to region, but each forum has key mandatory elements. Thus, meetings of Category 1 representatives of the aforementioned forums must be held at least once every 6 months; and their respective authorities have a duty to ensure interaction, cooperation, and sharing of information. The leadership and secretariats of local forums work on a continuous basis.

The approaches in each one of the four countries of the United Kingdom (England, Wales, Scotland, and Northern Ireland) to cooperation with the central government in emergency preparedness and response are slightly different. Still, the general rule is that protection of citizens' life and health, their property, and the environment are vested in the local governments within the territories of their responsibility. In turn, the tasks of counteraction to military, terrorist, and other national threats are vested in the central government. There are a number of pre-defined additional circumstances when the government of the United Kingdom can interfere in the emergency response at the level of local

communities. In particular, it includes large-scale emergencies involving one or more local communities in the region/country, where the impact cannot be mitigated by the local quick response services alone; emergencies that occurred at the national level or where the impact expanded from its focus to other regions/countries while the package of regional efforts and reserves is insufficient; emergencies arising from threats to national security (terrorism, acts of sabotage, external armed aggression, etc.); emergencies that occurred at critical infrastructure located on the territories of local communities, etc.

In general, in the United Kingdom and the Netherlands, the national resilience ensuring activities are conducted within a single cycle in a manner concerted at all levels. At this, special attention is paid to the establishment of inter-agency cooperation at all levels, partnership with businesses, and interaction with the population.

3.4.3. Comprehensive Approach to National Security and Resilience in New Zealand

The Government of New Zealand defines national security as the condition, which allows for the citizens to live with confidence, free from fear and with maximal use of all opportunities to improve their lives. To achieve this goal, it is necessary to ensure, first of all, protection and safety of human lives, property, and information. In New Zealand, the key threats are deemed to be inter-state (including armed) conflicts, transnational organized crime, cyber security incidents, natural hazards, biosecurity events, and pandemics (New Zealand Department of the Prime Minister and Cabinet, 2016).

New Zealand`s national security ensuring system makes emphasis on the resilience, which consists of the system's, people's, institutions', infrastructure's, and communities' ability to anticipate risks, respond to emergencies, contain their impact and eliminate their consequences, recover,

adapt, reorganize, learn from lessons of past experience and even prosper in changing conditions (Reznikova, 2020d).

To strengthen national resilience, New Zealand applies the all hazards – all risks approach, which envisages:

- reduction: identification and analysis of long-term risks and taking steps to eliminate them (if possible), reduction of their likelihood and the magnitude of their impact;
- readiness: preparation of systems and capabilities to counteract risks and emergencies before they happen;
- response: application of adequate effective measures before, during and after an emergency;
- recovery: coordinated efforts and processes for immediate, middle- and long-term recovery.

According to the aforementioned areas of activities, such an approach is also known as "4R" (reduction, readiness, response and recovery). The comprehensive approach to risk identification, and response requires an integrated, flexible, and adaptable architecture of the national security ensuring system capable of forming partnerships between governmental institutions, local authorities, private businesses, and citizens.

So, New Zealand`s national security ensuring system is built upon the following guidelines:

- it has to address all essential risks for citizens and state;
- its goals have to be achieved in a way stipulating government's accountability and responsibility for protection of the state, population, and national interests while respecting civil liberties and rule of law;
- decisions have to be made at the lowest appropriate level with coordination at the highest necessary level;

- the state has to maintain independent control of its own security strengthened by compliance with the international law and partners' support (New Zealand Department of the Prime Minister and Cabinet, 2016).

Comprehensive ensuring of national security in New Zealand contemplates achievement of the seven key goals of the state:

- to ensure public safety;
- to preserve sovereignty and territorial integrity;
- to protect lines of communication;
- to strengthen international order to promote security;
- to ensure sustainable economic prosperity;
- to maintain democratic institutions and national values;
- to protect the natural environment (New Zealand Department of the Prime Minister and Cabinet, 2016).

New Zealand develops the National Disaster Resilience Strategy, which partially is a Plan of implementation of the Sendai Framework for Disaster Risk Reduction (New Zealand Government, 2019b; United Nations, 2015a). The aforementioned National Strategy identifies the following priorities in the area of building resilience to disasters:

- managing risks;
- effective response to and recovery from emergency (including, in particular, building capability and capacity to manage emergencies);
- enhancement of community resilience (including, in particular, development of resilience and interaction culture).

In addition, this document defines the main areas to ensure resilience in New Zealand, including, among others, the following:

- social resilience (including promotion of social connectedness and cohesion, support to socially important functions, enhancement of social and human capital, etc.);

- cultural resilience (including preservation of cultural values, institutions, practices that identify the states, its history and heritage);
- economic resilience (including protection and continuity of businesses, financial markets, macroeconomic environments, etc.);
- resilience of the built environment (including protection and resilience of critical infrastructure, building and housing, engineering structures and facilities, urban planning, etc.);
- resilience of the natural environment (including sustainable and safe use of natural resources, land, adaptation to long-term climate change, etc.);
- governance of risk and resilience (including state policy, strategy, legislation, leadership, oversight, coordination, collaboration, etc.);
- dissemination of knowledge (including scientific research and actual information on risks and effective resilience practices).

Managing risks for national security and the states` and society's resilience enhancement is a complicated process, in which various public institutions participate. Local governments, non-governmental organizations, and the private sector of New Zealand play consistently a more important role in ensuring national security and resilience, in particular, at the strategic level, as well as in promotion of public awareness.

The state uses unified governance and coordination mechanisms in both normal and crisis conditions. The main attention is paid to mitigation of typical risk impacts rather than specific threats. This means that the experience gained in managing a specific type of risk can be applied to other risks.

Main responsibility for the national security is vested in the New Zealand central government:

- under normal conditions, it makes sure that the state policy, institutions, regulatory framework and resource distribution contribute to sustaining economic growth;

- under crisis conditions, it ensures management aimed at minimizing the negative impact of any deviations from the economy and society's normal functioning, interruptions in provision of critical goods and services and quick return to normal functioning of the state and society (New Zealand Department of the Prime Minister and Cabinet, 2016).

New Zealand Prime Minister simultaneously plays the role of security and intelligence minister while the National Security Group was established within the Prime Minister's Department and Cabinet of New Zealand to ensure general control, coordinate activities and support the national security ensuring system (New Zealand Department of the Prime Minister and Cabinet, 2021c).

New Zealand`s national security ensuring system is sufficiently flexible, which allows for quick and effective response to threats whilst in certain cases management can be implemented by inter-agency groups composed of officials of a respective level. When strategic planning or response at the national level is required, the management is undertaken by the Prime Minister and senior members of the Cabinet. A significant part of security responsibilities is entrusted to the local authorities.

National level response is implemented:

a) in case of threats that:

- are of extraordinary in scale, nature, intensity or potential impact;
- constitutes challenges to the sovereignty or nation-wide law and order;
- generate multiple or interrelated problems which constitute in their integrity a national or systemic risk;
- have such a high degree of uncertainty or complexity that the required response capabilities are in possession of the central government only;
- generate interdependent problems with potential cascade effect or escalation;

b) also, in the case of:

- threat response requires significant resources;
- there is ambiguity over who has the lead in managing risk, or there are conflicting views on solutions;
- the initial response is inappropriate or insufficient from a national perspective;
- involvement of different agencies is required;
- there is potential to enhance national security (New Zealand Department of the Prime Minister and Cabinet, 2016).

Inter-agency coordination and management at the national level do not override the powers and responsibilities of ministries as provided by the law. Their heads remain responsible for their activities and implementation of policies in the respective domain. In general, the goal of ensuring New Zealand`s national security is to establish effective coordination of the actors' interactions to solve complicated problems.

The government undertakes emergency management within the national security field in the case when the risk impact can lead to crises, events, or circumstances, which will have a systemic negative impact on key areas of the national security, in particular:

- public security;
- sovereignty, reputation, or critical interests abroad;
- economy or environment;
- effective functioning of the community (New Zealand Department of the Prime Minister and Cabinet, 2016).

New Zealand created the Coordinated Incident Management System [CIMS]. Its main objective is to ensure vertical and horizontal coordination of institutions and organizations through:

- establishing common structures, functions and terminology in a framework that is flexible, modular, and scalable so that the framework can be tailored to specific circumstances;
- support of institutions and organizations with a methodological framework, which they can use to develop their own emergency management processes and procedures that ensure both execution of their powers and interaction with other organizations (New Zealand Government, 2019a).

In New Zealand, readiness is ensured and emergencies are responded to according to the Civil Defense Emergency Management (CDEM) Act, National Civil Defense Emergency Management Plan Order, and other documents (New Zealand Legislation, 2002, 2015). The legislation defines the main types of emergencies, as well as the functions and responsibilities of central and local civil protection authorities (including national and local controllers and their groups); also, it is established that the main goal of risk management in New Zealand is the protection of the public and property against all kinds of threats. There are separate documents regulating issues of joint planning, situation monitoring, use of resources, communications, and other aspects of interaction in the respective domain, etc. (New Zealand Government, 2019a).

New Zealand has tight cooperation with other states in various aspects of resilience and security (in particular, with respect to foreign military presence and humanitarian assistance), and also, with regional and international organizations (APEC, ASEAN, Pacific Community Secretariat, UN and others).

In view of the above, it can be affirmed that New Zealand applies the comprehensive approach to ensuring national security and resilience, which stipulates that the resilience principles are implemented in all sectors of the national security and public governance including economic, social, environmental, public, international, and other domains. National resilience

management mechanisms are pinpointed by a wide cooperation, partnership, and public interactions framework.

3.4.4. National Risk Assessment Systems in the United Kingdom, the Netherlands, and New Zealand

National risk and threat assessment systems of the United Kingdom, the Netherlands, and New Zealand have been selected for this analysis because of specific reasons (Reznikova et al., 2020). The United Kingdom and the Netherlands have the most comprehensive systems. They cover the full cycle of assessing risks and capabilities, identifying threats and vulnerabilities, and preparing strategic decisions at various levels. New Zealand assesses risks, simulates crises, increases response readiness, manages crises, and recovers within a single cycle. Effectiveness of the national security and resilience ensuring model by New Zealand proved its effectiveness during response to the COVID-19 pandemic.

In **the United Kingdom,** the risk assessment system allows for the national security strategic planning, enables the government to assess a wide range of risks and threats to the national interests and security within the spectrum of short- and long-term changes in the security environment, identify strategic goals and priority objectives to ensure national security and resilience.

The risk assessment process involves means and assets of ministries and agencies, research and expertise institutions of the respective profile, local authorities, businesses, civil society, etc. The system operates in a comprehensive and consistent manner, within the single national security strategic planning cycle and algorithm. In course risk assessment, the governance hierarchical structure of the system applies the “top-down” principle, which means that the national risk assessment and threat identification makes a basis for respective activities at the regional and local levels.

For a long time, the United Kingdom has been conducting National Risk Assessment on a national scale (primarily, natural, man-made, biological and social risks), which can manifest themselves within the next five years. The results of the assessment are presented as a classified report. This document is the basis for the development of the UK National Security Strategy and for planning national resilience activities (UK Government, 2010).

National Risk Register [NRR] of Civil Emergencies is the public available version of the aforementioned report on comprehensive risk assessment (UK Government, 2017).The NRR has been developed since 2008. It is designed to inform the UK society about the actual risks, their manifestations, and impacts with the purpose to increase public awareness and preparedness for emergencies.

The National Risk Register is published every two years after the risk assessment results have been updated. From time to time, it changes its structure. As a rule, the document contains:

- review of main types of emergencies that can occur within the next five years (first of all, those defined in the UK Civil Contingencies Act, 2004);
- combined typical and high-priority emergency risk matrix (graded by likelihood/impact);
- features of emergency risks manifestation and their potential impacts;
- measures taken or planned by the central governments to overcome emergencies including contact information, phones, websites, and communication channels with authorized bodies;
- main provisions of the risk assessment methodology.

Based on the National Risk Register, regional risks are assessed and regional risk registers are prepared within the framework of local resilience forums activities, including within England, Wales, Scotland, and Northern Ireland. Actually, the National Risk Register is a point of reference and

methodological guide for local communities in the process of their regional risk registers and risk management systems.

In general, the practice of preparation and periodic update of the National Risk Register is of major importance for ensuring national resilience. This document is an important guide in contingency planning for entities such as communities, businesses, institutions, and more. Besides, it provides an opportunity to conduct timely outreach work among the population, preparing it for the possible occurrence of a certain emergency situation, which allows for strengthening the individual resilience of each citizen.

The National security risk assessment was conducted for the first time in course of preparation of the National Security Strategy and Strategic Defence and Security Review 2015, which established that such an assessment had to cover both domestic and external risks that can be identified within a period of five to twenty years, and had to be updated every two years. The document notes that the risk assessment results are not a prediction because the exact source and nature of future threats cannot be anticipated, but still makes it possible to set priorities to solve problems relevant to the state and society, as well as to form plans and resources required to respond to major risks (UK Government, 2015).

An important place in the UK strategic planning system belongs to the *national security capability assessment,* which is conducted within the National Security Capability Review (UK Government, 2018). Capability analysis allows determining not only their condition and sufficiency for effective response to threats, but also progress and problems in the implementation of the National Security Strategy and other program documents.

A key role in the institutional support of the risk and threat assessment system belongs to the UK Cabinet Office. At the beginning of the next assessment cycle, it assigns to the authorized ministries and agencies responsibility for analysis and assessment of a certain range of risks (grouped category of typical risk) in accordance with their competence. Preliminary

assessments are studied, new risks and threats are identified as well as those that have been identified before but have lacked the sufficient evidence base. Each ministry and agency describes scenarios of evolvement of the identified risks and threats, develops a grounded worst-case scenario for the typical risk (risk group) assigned to the authorized body. To fulfill this task, ministries and agencies create target working groups that follow guidelines received from the Cabinet Office with respect to risk assessment procedures and methodology.

If any risks are beyond the competence of any ministry or agency (so-called "cross-cutting" risks), they are assessed by the Cabinet Office Secretariat with participation of the Risk Assessment Steering Group within the Cabinet Office. Besides, the task of the Risk Assessment Steering Group is to concert current issues between ministries and agencies during an assessment. Also, this institution reviews assessments of new risks or any changes in those that have been assessed before.

Risk assessments and threat identification are conducted with assistance of other governmental institutions, in particular: Joint Terrorism Assessment Centre, Centre for the Protection of National Infrastructure, National Cyber Security Centre, Environment Agency, Met Office, and others.

An important place in the UK risk and threat assessment system is given to *scientific-methodological support* of this activity. The Government Office for Science plays the role of an independent arbiter on scientific and technological matters of the risk assessment. The Scientific evaluation of the assessment results is conducted by a group of scientific advisors for emergencies headed by the Government Chief Scientific Adviser who at the same time is the head of the Government Office for Science and Co-Chair of Prime Minister’s Council for Science and Technology.

Advisory support for the national risk assessment and threat identification is implemented by the Natural Hazards Partnership. This is an independent community created to exchange best practices, develop recommendations for the

government and the public with respect to risk assessment, model their impacts and resilience ensuring mechanisms, establish communications and ensure stakeholders' interactions. For now, the Natural Hazards Partnership includes 17 specialized governmental institutions.

In the **Netherlands,** a comprehensive risk and threat assessment system is an important element of strategic planning and a tool to develop a National Security Strategy. It embraces a number of processes including, among others, the following: security environment assessment, risk and threat assessment, identification of the security situation long-term trends, and capabilities assessment.

In general, adoption of the Dutch National Security Strategy initiates a strategic cycle, which iterates every three years and allows for continuous assessment of whether national interest protection activities remain sufficiently effective to respond to all risks and threats that can affect the national security (The Netherlands National Coordinator for Security and Counterterrorism, 2019b). Results of the periodic risk assessment are presented in such reports as National Risk Assessment or National Risk Profile (The Netherlands National Coordinator for Security and Counterterrorism, 2019c; The Netherlands National Network of Safety and Security Analysts, 2016). In contrast to the National Risk Assessment, in addition to assessment of risks for basic national interests and their impact, the National Risk Profile also contains an assessment of the state's capabilities to respond to the threats. Such reports are expected to be prepared every four years (The Netherlands National Network of Safety and Security Analysts, 2018).

Dutch National Security Strategy defines the following security interests:

- territorial integrity;
- physical security;
- economic security;
- environmental security;

- social and political stability;
- maintenance of the international peace and order (The Netherlands National Coordinator for Security and Counterterrorism, 2019b).

In general, National Risk Assessment Report contains:

- description of the key risks by certain their group profiles (or area), analysis of factors and events that can influence formation of a certain threat, as well as of causes, triggers, interlinks, and interdependencies of the risks;
- identification of the risks which will have the biggest impact on the national security interests;
- description of risk and threat manifestation scenarios;
- assessments of risk and threat likelihoods and impacts;
- identification of categories of similar and interrelated risks (for example, those targeting the same group and having similar nature, etc.);
- identification of priority risks;
- recommendations on risk reduction (their likelihood and impacts).

The latest National Risk Assessment Report was prepared in support of the National Security Strategy development (The Netherlands National Coordinator for Security and Counterterrorism, 2019c).

Risk analysis, assessment and prioritization methodology, which is used to prepare the National Risk Profile, is similar to the one used to develop the National Risk Assessment. Risks are assessed by both likelihood criteria and their impact on the national security key interests. In the course of the risk analysis, the general situational context and long-term megatrends are considered, causes, triggers, influence factors, cascading effects of a threat are examined, anticipated scenarios are developed, etc. Besides, there is assessment of the available capabilities to prevent, prepare for response, control the situation, respond to and mitigate the impacts of any threats; vulnerabilities are

identified; uncertainty impact is assessed. With consideration of the produced results, conclusions and recommendations are developed with respect to enhancement of capabilities and national resilience development. As of now, the Netherlands has developed and published only one National Risk Profile (The Netherlands National Network of Safety and Security Analysts, 2016).

The Netherlands National Security Strategy defines the following general priorities for national security risk and threat assessment:

- threat from actors sponsored by other states;
- society polarization;
- damages to critical infrastructure;
- terrorism, extremism;
- military threat;
- crime;
- cyber threat (The Netherlands National Coordinator for Security and Counterterrorism, 2019b).

Based on the analysis of risks and threats, this document recommends:

- enhance multilateral international interaction mechanisms and systems, including through conclusion of the relevant international treaties and improvement of the international law provisions;
- increase the level of preparedness for potential natural disasters;
- prevent and increase the level of preparedness to respond to potential man-made disasters (first of all, chemical, biological, radiological, and nuclear);
- prevent and increase the level of preparedness to respond to potential spread of contagious diseases (The Netherlands National Coordinator for Security and Counterterrorism, 2019b).

In addition to the preparation of the risk assessment results report, the strategic planning cycle also includes interim scanning of the national security horizon, which envisages analysis of national security trends and threats from

the point of view of whether any changes should be introduced in the Dutch National Security Strategy (The Netherlands National Coordinator for Security and Counterterrorism, 2019b). The scanning allows for finding new megatrends, which would last for at least five years (The Netherlands National Network of Safety and Security Analysts, 2019).

Also, Dutch National Security Strategy defines the need to establish a general risk and crisis management system as an important mechanism to ensure national security. Besides, it emphasizes the importance of the use of scientific research with respect to risks and threats, as well as new risk monitoring technologies for national security (The Netherlands National Coordinator for Security and Counterterrorism, 2019b).

To ensure scientific-methodological support for the risk and threat assessment processes and to prepare the appropriate reports, the Netherlands established the Network of Analysts for National Security (2018). It includes six continuously operating organizations, namely: National Institute for Public Health and the Environment [RIVM] within the Ministry of Health, Welfare and Sport of the Netherlands; Research and Documentation Center [WODC] within the Ministry of Justice and Security; General Intelligence and Security Service of the Netherlands [AIVD] within the Ministry of Interior; The Netherlands Organization for Applied Scientific Research [TNO]; The Netherlands Institute of International Relations 'Clingendael' Erasmus University Rotterdam, Institute of Social Studies [ISS]. If necessary, other educational institutions, research organizations, civil services, representatives of the Security Regions, critical infrastructure enterprises, private companies, consulting companies, etc. can be involved in the Network's activities. In particular, an active participant in the Network is The Hague Center for Strategic Studies (HCSS)[22].

[22] *The Hague Centre for Strategic Studies*. https://hcss.nl/

Within the Network, subject-matter inter-agency working groups can be formed so that each one of them would analyze and assess a certain risk category. Such groups include researchers and analysts specializing in risk assessment and anticipated scenario development, experienced experts from the profile ministries and agencies, and other specialists.

The Network activities are supported by the Secretariat, which functions continuously within the National Institute for Public Health and the Environment. The secretariat coordinates activities of the Network permanent participants and temporary working groups, manages projects and monitors their progress, and supports interaction with the Task Group and state authorities that coordinate the Network activities at the strategic level. They include National Security Steering Committee (*Dutch:* Stuurgroep Nationale Veiligheid); Interagency Working Group For National Security (*Dutch:* Werkgroep Voor Nationale Veiligheid) reporting to the aforementioned Steering Committee; Ministry of Justice and Security and National Coordinator for Security and Counterterrorism which operates within this Ministry.

The Network also includes the National Risk Assessment Methodology Working Group (*Dutch:* Methodiekwerkgroep Nationale Risicobeoordeling) established within the Ministry of Justice and Security of the Netherlands. Its activities are supported by the Analysis and Strategy Division, which operated under the leadership of the National Coordinator for Security and Counterterrorism within the aforementioned Ministry. The Methodology Working Group, among other topics, analyzes compliance with the general methodology of the risk and threat assessment approved in the state in 2007.

Research with respect to the risk and threat assessment is conducted and relevant reports are prepared by the Network in tight cooperation with Security Regions.

The Netherlands Scientific Council for Government Policy conducts the final expert examination of the draft National Risk Assessment and National

Risk Profile before they are presented to the Netherlands government and parliament for review.

In addition to the risk and capabilities assessment, the state also assesses the effectiveness of the national security legislation including areas of crisis management and legal support to Security Regions, checks preparedness of the public and state to effectively respond to crises.

In general, the Netherlands' national risk and threat assessment system is constantly being improved, which allows it to be further adapted to changes in the strategic security environment. Today it is implemented in a comprehensive and consistent manner by a single algorithm within the national security strategic planning cycle.

New Zealand has been assessing risks for decades. Within this process, they analyze all potential risks and threats: domestic, external, man-mad, natural, and others.

With the leadership of the Prime Minister and the Cabinet of Ministers [Cabinet] of New Zealand and with consideration of the international experience, a general national risk assessment and management methodology was prepared. It is based on the Standard AS/NZS ISO 31000.2009 developed jointly with Australia on the basis of ISO 31000 (New Zealand Standards, 2009). This Methodology defines main procedures and stages of the risk and threat assessments, as well as current and prospective risk management options.

The New Zealand national risk assessment system involves a wide range of actors and their interaction with the local authorities, non-governmental organizations, and the private sector. For purposes of the risk assessment, the experience of relevant governmental organizations is used, the obtained information is analyzed, technical expertise of capabilities is performed, etc. Such activities are implemented with support of scientific research institutions. Risks are assessed, risk profiles and crisis evolution scenarios are developed and reviewed under supervision of a working group composed of the governmental

officials. The focus is on awareness and management of general risk consequences and vulnerabilities, rather than specific hazards.

New Zealand assesses the risks of both emergencies and those for the national security. In particular, the Department of the Prime Minister and Cabinet renders organizational and informational support to the public authorities responsible for assessment of the most significant risks to the national security in order to find options for their mitigation and to identify ways to enhance the national resilience. These activities are pinpointed by a special mechanism, which ensures a proactive and concerted approach of all governmental entities to the risk identification and management (National Risk Approach) (New Zealand Department of the Prime Minister and Cabinet, 2021a).

New Zealand established the National Assessments Bureau, which produces an independent and unbiased assessment of events and trends related to national security and foreign relations. Such assessments are used to form national security and resilience policy. The assessments may differ: some of them identify the likely trajectory of imminent national or regional crisis evolution and its consequence, while others focus on long-term and strategic issues, in particular, such as global security trends. The National Assessments Bureau is an integral part of the New Zealand national intelligence community (New Zealand Department of the Prime Minister and Cabinet, 2020b).

According to the national approach to risk management, the National Intelligence and Risk Coordination directorate maintains the classified National Risk Register. It contains a wide range of hazards and threats across the following main domain:

- natural hazards;
- biological hazards;
- technological hazards;
- malicious threats;

- economic crises (New Zealand Department of the Prime Minister and Cabinet, 2021a).

Risks are also identified and analyzed at the regional and local levels. Risks are assessed on a comparative basis with respect to a middle level of threat for the whole country. Based on the obtained results, risk and threat profiles are developed, which define practices for managing them at different stages (risk reduction, preparation, response and recovery). In turn, the developed risk profiles are used to plan the relevant activities.

In addition to the central and local authorities, non-governmental and private actors (infrastructure owners/operators, small and medium size businesses, researchers) participate in the risk assessment and management. Such participation is mostly voluntary, although there are a number of legislative requirements for the critical infrastructure owners (energy supply, telecommunications, etc.) with respect to availability and continuity of their services.

The risk assessment organized in this manner allows for the central governmental institutions to identify gaps in the data received for analysis or in their understanding of the essence and manifestations of certain risks and also enhances confidence in the reliability of the assessment results which constitute the basis for development of the action plans to ensure readiness to respond to threats, determination of state`s priorities in national security, etc. (New Zealand Department of the Prime Minister and Cabinet, 2021b).

New Zealand's experience shows that there is usually a lack of reliable quantitative data to assess the most serious risks, so it is advisable to use qualitative indicators that characterize the nature of the risk. Some of the impact types cannot be assessed in a systemic manner because of complicated cascade effects or when their combinations have been defined wrongfully (for example, economic, societal, environmental, and reputational impact). Such situational or contextual impact elements and factors can significantly strengthen and

supersede the anticipated impact. Impact assessment also takes into consideration the effect of preventive or preparatory activities used for risk mitigation.

New Zealand National Disaster Resilience Strategy identifies a set of measures to counteract disasters and ensure national resilience as one of the priorities of the state's activities (New Zealand Government, 2019b). Among the suggested measures, the following should be mentioned:

1) to identify risk evolution scenarios (including consideration of risk components, impacts, vulnerabilities, and capabilities) and methods to use this information for governmental decision-making;

2) to establish governmental institutional entities in the area of risk management, to determine procedures and take measures required to mitigate the risks;

3) to ensure awareness of the society and governmental institutions with respect to the risks, to develop capabilities for their assessment and management;

4) to remove flaws in the state policy in risk reduction;

5) to implement information policy aimed at the public awareness of the existing risks and prevention of new ones;

6) to develop and enhance the national resilience ensuring mechanisms.

General information on risks and threats is available to the public, central and local government authorities, as well as scientific research institutions (except for classified data). In order to inform the population, a publicly available version of the New Zealand National Risk Register dealing with the risk assessment and identifying state policy priorities in emergency response is used. In 2019, a new web-site Get Ready was launched granting wide access to the information related to ensuring emergency response readiness and ways to enhance the national resilience (New Zealand Department of the Prime Minister and Cabinet, 2020a).

The State's leadership identifies as an important task to master the lessons learned from the national risk assessment and their consideration for purposes of the new data analysis within the new assessment cycle.

According to the government estimates, a small country with well-developed infrastructure and a relatively strong tradition of cooperation between ministries and agencies has fewer difficulties in identification and involvement of different stakeholders in the assessment process. The state is able to assess the security situation and solve the identified problems, although its weakness is the trend to underestimate uncertainty, complexity, and ambiguity of the risks (New Zealand Department of the Prime Minister and Cabinet, 2019). In addition, the most serious risks are, as usual, the least known whilst the worst ones are those that are not known at all. The proof is the COVID-19 pandemic.

In general, national risk and threat assessment systems of the studied states are organized on the basis of a whole-of-government interaction and cooperation with other actors. Their activities incorporate provisions of international standards (ISO) concerning crisis and risk management. Also, these systems strike an optimal balance between pragmatic governance and scientific research results.

Conclusions to Chapter 3

Uncertainty of the global security environment, the need to confront hybrid threats and hazards related to the development of new and cutting-edge technologies have intensified the search for new approaches to ensuring national security and resilience at the level of both states, and their alliances and international organizations. New practices are actively implemented and the existing practices and mechanisms are enhanced, which allow for the states and their societies to enhance their ability to adapt to changing security environment without significant losses, react in a timely and effective manner to the wide

spectrum of threats and crisis situations, which are becoming more difficult to identify, enhance different actors' capabilities, organize cooperation between them, etc.

The results of the study of the foreign experience in ensuring national resilience demonstrate that the leading international organizations and alliance of nations raise their attention to strengthening their national resilience or its specific aspects. The research domain, selection of the resilience actors, and orientation of the relevant practices depend on the organization's main direction and experience of the involved experts. Goals and objectives identified by the UN, NATO, EU, OECD, and OSCE in the area of ensuring peace, security, prosperity, sustainable development, and partnership in different countries of the world contain numerous activities fostering building national resilience in different countries. In particular, such activities are aimed at eliminating conflict causes, forming cohesion, trust, leadership, implementing the comprehensive approach to providing preparedness for and effectiveness of the response to a wide spectrum of threats, quick recovery after crisis, etc.

It can be stated that the main activities of international organizations to build resilience are the study of existing national practices, analysis, and development of recommendations for states on various issues of national resilience, providing expert, organizational, financial, and other support to countries in need. Within such activities, special attention is paid to risk analysis, identification of vulnerabilities, awareness enhancement, crisis management development, establishment of a whole-of-government and whole-of-society cooperation, ensuring readiness to threat response and recovering after crises, action planning, etc.

After 2014, some changes are observed in approaches of the international organizations and states alliances to the national resilience, definition of priority areas, and directions of its enhancement. The conducted analysis of strategic and program documents and practices of studied international organizations and

states alliances in the resilience domain allows for stating that in general they are aimed at achievement of the resilience criteria of the state and resilience criteria of the functioning of the state and its subsystems. At the same time, a significant part of the activities implemented by the international organizations and states alliances in this area also contribute to enhancement of society`s resilience and achievement of such results as forming of identity, cohesion, and unity; strengthening of linkages between various societal groups and trust to the government; engagement of the public in economic, political and other activities within communities and the state, as well as enhancement of effectiveness of the community governance; awareness of citizens concerning the nature and character of threats and action plans in case of their manifestation; enhancement of readiness to respond and controllability of the situation before, during and after crisis; creation of joint capabilities to overcome threats and crises.

It should be noted that the fight against the COVID-19 pandemic raised new issues in the world with respect to crisis management and the post-crisis recovery, planning, and implementation of the concerted activities, investments into resilience, etc. International organizations and states alliances continue working in this direction.

As proven by the world experience, the specifics of development and implementation of the state policy in national security and resilience, as well as peculiarities of creation of appropriate systems in different countries are to a big extent stipulated by their national interests, historic, geographic, security, political, cultural, socio-economic and other conditions of state formation and development. At the same time, national resilience ensuring models formed in different countries have many common features because all of them are based on regularities and essential characteristics of the national resilience concept.

As a rule, states started using the resilience-building mechanisms within their priority areas, where the risks were assessed as the most likely and their impact, as of the largest scale and harm to the state and society. With the time,

directions and domains for ensuring national resilience were specified and expanded while the relevant practices were developed. The main changes that now are observed in the national resilience ensuring systems of many states are moving from concentration on priority domains towards the comprehensive approach to ensuring resilience to various threats based on the whole-of-society cooperation. At the same time, states' priorities in the national resilience and directions of the respective mechanisms and practices may vary significantly.

In the context of effective application of the national resilience ensuring mechanisms such as strategic planning, comprehensive risk assessment, threat and vulnerabilities identification, multi-level organization of the overarching cooperation to provide national security and resilience, etc., the experience of the United Kingdom, the Netherlands and New Zealand deserve attention.

In general, examination of the world experience in ensuring national resilience, analysis of effective practices in this area, different approaches to organization of the national resilience ensuring system, and key processes in this domain allow making the best choice for Ukraine to determine the national resilience ensuring model with consideration of the national interests and peculiarities of the state development.