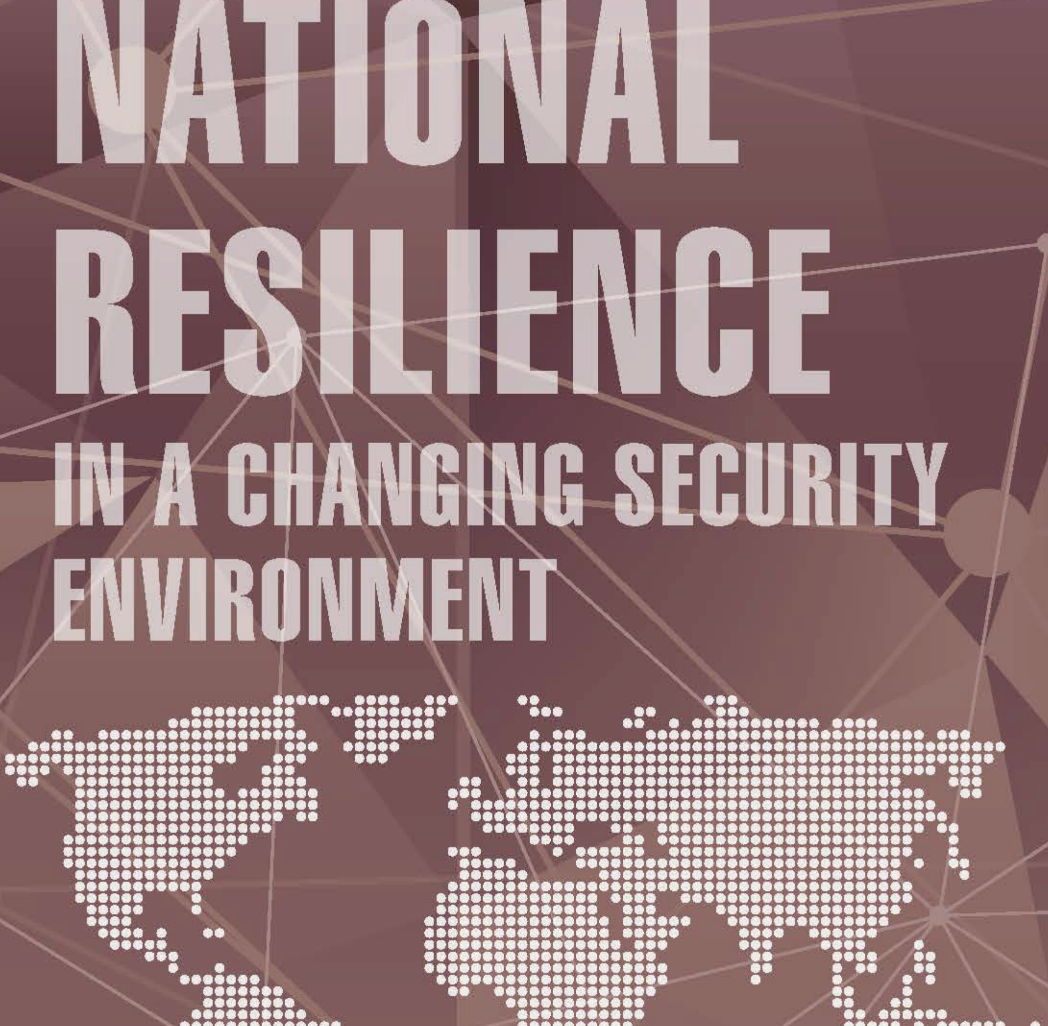
Olga Reznikova

NATIONAL RESILIENCE

IN A CHANGING SECURITY ENVIRONMENT



Scientific publication

Olga REZNIKOVA

NATIONAL RESILIENCE
IN CHANGING SECURITY ENVIRONMENT

Monograph

Design by Pavlo Reznikov

The monograph was prepared for publication
at the National Institute for Strategic Studies
Pyrohova str., 7-a, Kyiv, 01030
Tel./fax: (044) 234-50-07
e-mail: info-niss@niss.gov.ua http://www.niss.gov.ua

CONTENTS

INTRODUCTION

Relevance of the study. The modern world is undergoing large-scale transformations in almost all areas of social relationships. Recently, climate change factors have become significantly more influential, new dangerous diseases have become widespread, the anthropogenic burden on the environment has increased, the Fourth Industrial Revolution is rapidly unfolding, and production is actively dematerializing. The global security environment features high turbulence and unpredictability, the international system of strategic stability is collapsing, competition between states is escalating, and emerging conflicts are increasingly difficult to resolve.

Strengthening national resilience can be an effective response to current challenges. Forming and implementing the relevant public policy direction better addresses threats of any origin and nature, including hybrid, to adapt to abrupt and unpredictable changes in the security environment, maintain sustainable functioning of the state before, during, and after crisis and quickly recover to balance optimally under the determined conditions. And in general – to endure (or even sometimes survive), and reduce losses in immensely complicated (crisis) circumstances that cannot be avoided.

These results can be achieved by providing the appropriate level of state and societal readiness to respond to a wide range of threats and dangers, timely detection of vulnerabilities that weaken security capabilities, to carry out adaptive management, effective crisis management and liaison at all levels, create necessary reserves and alternative strategies, plan measures and implement universal protocols of coordinated actions, disseminate necessary knowledge and establish reliable communications, rationally use resources, etc. Everything mentioned determines priority directions and tasks in forming the national resilience ensuring system, which still needs to be formed in Ukraine.

Today, Ukraine faces a range of threats of both external and internal origin. Hybrid threats, which are particularly difficult to detect, are a major concern. Their coordinated and simultaneous application in various fields is very dangerous for both the state and society. Countering these threats requires significant financial, technical, and human resources limited in most countries, especially in Ukraine, which has recently suffered significant material and human losses due to aggression by the Russian Federation.

Under modern conditions, the resilience capabilities of the state and society as complex systems need development and adaptive management. The national resilience ensuring system is intended to perform these functions. Some of its mechanisms are applied in Ukraine. However, their comprehensive implementation based on a systematic approach requires some changes in the elaboration of state security policy, improving organizational and legal support in the fields of national security and public administration, streamlining liaisons between existing and emerging nationwide systems (civil protection, countering terrorism, health care, social protection, cybersecurity, law enforcement, banking, etc.), providing proper cooperation and synergy of security and defense forces, state and local authorities, business and civil society, establishing effective coordination of their activities, and implementing principles of resilience in various fields, especially national security.

Building up a national resilience ensuring system will enable performance of adaptive management of the state and society’s resilience in accordance with the determined performance benchmarks and criteria. What is crucial here, is not establishing new state bodies and institutions, but strengthening the resilience of the existing ones and forming reliable links between all national resilience providers. To do this, a new paradigm of thinking should be introduced, stereotypes should be overcome, security culture developed, society consolidated, joint countering to a wide range of threats ensured, and responsibility and mutual assistance in the society formed.

A national resilience ensuring model depends on state needs, the state's participation in certain international organizations and alliances, and other factors. Different countries have quite different experiences in this area. There is no universal model to meet everyone's needs. Mechanisms and practices that have been sufficiently effective in some countries may not meet the conditions and needs of others. Learning from the experiences of other countries and recommendations of leading international organizations will enable the implementation of best world practices with due account for national interests and specific developmental characteristics of the Ukrainian state and society. At the same time, proper scientific substantiation of the chosen conceptual framework, model, and mechanisms will help avoid mistakes while forming and implementing new complex projects. Creating a national resilience ensuring system is, in particular, such a project for Ukraine.

Degree of scientific development of the topic. National resilience studies have an interdisciplinary nature and require an understanding of theoretical foundations in certain scientific directions.

Studies in *systems theory*, including complex systems (represented primarily by the works of R. Ackoff, L. von Bertalanffy, O. Bogdanov, J. van Gigch, E. Vinogray, W. Ashby, T. Parsons, N. Ovchinnikov, I. Prigozhyn, Yu. Sachkov, M. Setrov, W. Scott, I. Stengers, and A. Uyemov) are extremely important to understanding the concept of resilience and forming systematic mechanisms to ensure national resilience.

Aspects of the *interdisciplinary resilience concept* development and the new approach to scientific research of resilience thinking are covered in the works of the following scientists: T. Abel, W. Adger, K. Barrett, F. Berkes, M. Biggs, E. Boyd, K. Brown, F. Brand, W. Brauch, W. Galas, K. Jucks, J. Ebbesson, K. Eckerberg, A. Duit, S. Carpenter, J. Colding, M. Constas, T. Crane, C. Curtin, C. Lyon, K. Magis, M. Mitchell, D. Nelson, E. van Ness, A. Norström, O. Olsson, J. Parker, S. Polasky, S. Robinson, J. Rockström, H. Ross,

J. Stepp, H. Özdemir, G. Özkan, T. Hughes, J. Hodicky, C. Holling, C. Folke, R. DeFreese, M. Schlüter, M. Schoon, and others. The concept of resilience has gradually become an integral part of sustainability science.

Many researchers including J. Anderies, K. Wyche, W. Wolford, M. Walsh-Dilley, M. Cooper, P. Martin-Breen, F. Norris, B. Pfeferbaum, R. Pfeferbaum, S. Stevens, J. Walker have focused on the diversity and transformation of the resilience concept. The relevant research was also conducted by some scientific and public institutions, including the Community and Regional Resilience Institute [CARRI].

The works of such known worldwide scientists as M. Barnett, T. Balzacq, D. Bezvik, A. Bellamy, K. Buz, B. Buzan, T. Weiss, O. Waver, P. Williams, J. Duffield, H. Dexter, D. Joseph, R. Jones, B. Evans, A. McGrew, J. Reid, S. Tang, E. Thompson, R. Ullman, D. Held, J. Hertz, J. Hoogensen Gjørv, L. Friedman, M. Foucault, D. Chandler, as well as such Ukrainian scientists as V. Abramov, O. Belov, V. Bogdanovich, V. Gorbulin, D. Dubov, B. Kaczynski, O. Kornievsky, V. Kosevtsov, V. Mandrageli, N. Nyzhnyk, O. Lytvynenko, A. Semenchenko, G. Sytnyk, and V. Smolyanyuk helped form and develop a separate scientific field of *security studies*.

Evolving conceptual approaches to national security, developing systems theory, and a separately forming resilience research direction let the resilience concept expand to the field of security research and form a *national resilience concept*. Among the researchers of this phenomenon are J. Anderies, P. Bourbeau, J. Joseph, B. Evans, C. Zebrowski, M. Cavelti, M. Kaufmann, K. Christensen, M. Cooper, P. Martin-Brin, G. Lasconjarias, V. Proag, J. Reid, J. Rensel, J. Walker, C. Fjäder, D. Chandler.

In recent years, the amount of applied research in various fields and directions of national resilience has significantly increased. In particular, this research highlights the experiences of different states in national resilience building, including particular details on the application of certain mechanisms of ensuring national resilience in various spheres of activity (economic, energy, financial, etc.), on the interaction of various social relations actors. In this context, important studies have been conducted by famous scholars H. Bole, I. Weissmel-Manor, J. Woods, R. Donno, B. Atzold, D. Canetti, M. Kick, R. Klein, N. Cohen, R. Nicholls, J. Pollack, K. Rapaport, F. Tomalla, and L. Francar. Among the Ukrainian researchers, the scientific works of A. Boyko, D. Dubov, V. Kopchak, M. Samus, O. Sukhodolia, and O. Pokalchuk are of interest.

Many studies examine *the processes and outcomes assessment methodology* in complex systems, among which the works of J. van Gigch, P. Ratush, Y. Kharazishvili, and Ch. Churchman are worthy of note. Issues of *planning* (including strategic planning) feature prominently in studies of universal resilience mechanisms, represented in the works of well-known scientists G. Eisenkot, I. Ansoff, H. Bandhold, A. Butcher, P. Dixon, G. Kahn, M. Lindgen, G. Mintzberg, J. Ringland, J. Steiner, J. Tam, P. Schwartz, and G. Shiboni, as well as Ukrainian scholars V. Gorbulin, A. Kaczynski, and G. Sytnyk. In general, according to Cavelti, Kaufmann, and Kristensen (2015), the number of publications on resilience registered in the international "Web of Science" database has increased significantly: from about 500 in 2003 to 3000 in 2013. According to estimates by Borisoglebsky, Naghshbandi, and Varga (2019), the number of such publications, selected only by certain search criteria, reached almost 350,000 in 2019. Currently, the Google search engine provides more than 170 million results for the "national resilience" query and more than 10 million results for the same query in Ukrainian.

At the same time, the issue of forming and functioning of the national resilience ensuring system is presented in the scientific literature only in fragments. The logic of choosing a national resilience ensuring model with due account for national interests and features of state and society development and filling this model with appropriate systemic mechanisms with due account for the cyclical nature of key processes and influence factors, as well as issues of determining the effectiveness of universal and special mechanisms of ensuring national resilience, and forming the relevant state policy have been studied insufficiently. Besides, there is now a widespread trend to manipulate the term of resilience in the field of national security, when unsystematic measures in separate areas are proposed under the guise of providing national resilience.

The above-mentioned aspects require proper scientific studies, and the relevant theoretical knowledge should be enhanced due to their high practical value in modern conditions. That is why it is scientifically and practically expedient to formulate and solve the topical ***scientific problem*** of developing conceptual, methodological, instrumental, and applied components of providing national resilience in a high-turbulent and uncertain security environment with due account for state and society development features.

In Ukraine, national resilience studies have begun not so long ago and currently have no systemic nature. The Ukrainian expert community has no common understanding of key terms, objects, subjects, directions, processes, criteria, and indicators of providing national resilience, which have an interdisciplinary nature. Despite a number of tasks set by government strategic and program documents on creating a national resilience system, there is no proper scientific substantiation for the conceptual framework of this process, choosing a national resilience ensuring model, key tasks to be solved, etc.

Given the above, as well as taking into account the topicality of the national resilience issue in modern conditions, it is crucial to develop scientifically validated recommendations on establishing a national resilience ensuring system in Ukraine.

The ***research object*** was forming and implementing public policy in national security and resilience.

The ***research subject*** was forming a national resilience ensuring system in modern Ukraine.

The ***research aim*** was to determine a scientifically validated conceptual framework and optimal ways of providing national resilience in modern Ukraine with due account for successful foreign practices. This implied the practical implementation of the resilience concept in national security through establishing the national resilience ensuring system in Ukraine.

To achieve this aim, a number of ***objectives*** should have been accomplished. In particular, it was necessary to:

determine the meaning of the interdisciplinary resilience concept, its characteristics, and manifestations;

characterize peculiarities of implementing the resilience concept in national security;

substantiate the expediency of a systems approach to national resilience;

generalize the conceptual framework of forming and functioning of the national resilience ensuring system, including its liaison with the national security ensuring system;

identify and characterize the basic principles, criteria, processes, and mechanisms for ensuring national resilience, which are interdisciplinary in nature;

analyze the specifics of formulating state policy in national resilience;

systematize and characterize key mechanisms for ensuring national resilience, including mechanisms of integrated risk and capability assessment, threat identification, vulnerability detection, adaptive management, a comprehensive multi-level organizational mechanism, etc.;

characterize the logic of choosing the national resilience ensuring model and its key parameters;

generalize foreign experiences in building national resilience from the perspective of identifying opportunities for its implementation in Ukraine;

analyze how the approaches to resilience-building used by international organizations and individual states have changed in recent years. This analysis should help identify opportunities for expanding cooperation of these organizations and states with Ukraine and implementing relevant recommendations while forming and implementing the state policy in national security;

characterize the current security environment of Ukraine and highlight its key trends in the context of determining the future national resilience ensuring system formation prospects;

analyze the current status and summarize the key problems of the resilience in national security of Ukraine;

substantiate the expediency of creating the national resilience ensuring system in Ukraine, to present the author's vision of its prospective model;

develop recommendations for determining the national resilience conceptual framework in Ukraine, building key system mechanisms, forming the relevant state policy, improving national legislation, etc.

Research methodology. The study was divided into several stages.

Initially, the scientific literature was reviewed and grouped according to the key research directions: the complex systems theory, resilience studies, and security studies. Given the need to describe and clarify the key system mechanisms and processes of providing national resilience, scientific works on risk assessment and management, identification of threats and vulnerabilities, formation and implementation of public policy, strategic planning, and public administration have been identified and analyzed.

Such methodological approaches and research methods as analysis and synthesis, systematic, system-structural, and structural-functional approaches, descending from abstract to concrete, induction and deduction, historical, logical, and other approaches used at this stage allowed the formation of a theoretical foundation for further research, namely: to determine a conceptual framework for the formation and functioning of the national resilience ensuring system, the logic of building a multilevel integrated model and universal mechanisms of ensuring national resilience, and national resilience public policy development features. At the same time, the patterns identified allowed us to clarify the basic definitions, identify systemic elements and links, determine the national resilience ensuring cycle, characterize criteria, indicators, and national security resilience levels that have an interdisciplinary nature and can form a framework for developing specific resilience indicators in various fields.

In the next stage of this study, the best world practices in ensuring national resilience have been reviewed and analyzed. To this end, implemented project results, analytical materials, regulatory documents, and recommendations of leading international organizations and alliances, including UN, NATO, EU, and OSCE as well as international standards in security and resilience of states, communities, organizations, and enterprises have been examined. Besides, different states' experiences in providing national resilience, creating the relevant systems and universal mechanisms, including national risk assessment systems, multi-level organizational support mechanism, etc. have been studied. In order to determine the peculiarities of forming the national resilience ensuring model, special attention has been paid to the relevant experiences of Great Britain, the Netherlands, and New Zealand. Analytical reports, regulatory documents, and information references not only of these countries but also of the United States, Japan, Israel, Sweden, Norway, Estonia, and other countries have been examined in order to discover key characteristics of functioning of universal and some special system mechanisms.

In addition to the above-mentioned methodological approaches and research methods, observations, comparisons, and analogies were used at this stage. This helped identify successful world practices that can be implemented in Ukraine.

The security environment of Ukraine and national resilience providing state were analyzed at the next stage. To this end, official statistical materials, analytical reports of public authorities, Ukrainian regulatory acts, especially in national security, civil protection, organizing activities of public and local authorities, as well as scientific publications and expert assessments published during numerous communication events have been studied.

Based on the analysis results, the key problems in providing national resilience in Ukraine have been identified. Taking into account the obtained theoretical conclusions, successful world experience, and the features of functioning and development of the Ukrainian state, society, and national interests, recommendations on the conceptual framework and optimal model to ensure national resilience in current Ukrainian circumstances, ways to improve preparation and implementation of comprehensive strategic decisions, as well as on national security planning, establishing a unified legal framework, and on defining basic terms and basic mechanisms in the field of ensuring national resilience have been developed. In addition, recommendations on the development of a range of draft regulatory documents, including a draft decision of the National Security and Defense Council of Ukraine to establish a National Security Risk and Threat Assessment Center and improve the work of the Main Situational Center of Ukraine, as well as amendments to the Law of Ukraine "On National Security of Ukraine," and the Civil Code of Ukraine have been formulated.

Therefore, the combination of theoretical and empirical research methods allowed not only to solve the determined scientific problems but also to form conclusions and significant practical recommendations for Ukraine.

The structure of the monograph was determined according to the above-mentioned logic of the research conducted during the preparation of this publication. The monograph consists of an introduction, five chapters followed by findings, general conclusions that emerged from the research results, a glossary, a list of references, and annexes.

The monograph has been drawn up according to the research plan of the National Institute for Strategic Studies on the following topics: "Strategic trends in global development and their impact on national security of Ukraine" (state registration number 0113U001153, 2013), "Current threats and challenges to Ukraine's national security in the context of globalization" (state registration number 0114U003203, 2014), "Improving the national security ensuring system of Ukraine" (state registration number 0115U003107, 2015), "Problems and ways of providing the national security of Ukraine in the face of increasing internal and external threats" (state registration number 0116U001471, 2016), "Countering separatism: conclusions for Ukraine" (state registration number 0117U4174, 2017), "Ensuring state resilience to national security threats" (state registration number 0118U003506, 2018), "Protection of national interests of Ukraine in the crisis of the security environment" (state registration number 0120U000260, 2020, state registration number 0120U000066, 2021).

The research results were validated during numerous scientific and scientific-practical conferences, workshops, and other communication events, including with international participation. Some research results have been practically implemented because the monograph's author worked in the interagency national resilience buildup working group, established under the Commission for the Coordination of Euro-Atlantic Integration of Ukraine, participated in the elaboration of a range of draft regulatory documents of Ukraine, including a draft Concept of Support of the National Resilience System and prepared analytical reports of the National Institute for Strategic Studies to the annual Address of the President of Ukraine to the Verkhovna Rada of Ukraine "On the Internal and External Situation of Ukraine" and other analytical documents.

Possible further research. Although national resilience studies are now performed quite actively, there are still possibilities for further research. Issues related to the integrated approach to sustainable development with due account for security and resilience, improving the risks and threats assessment methodology, as well as resilience in certain areas, building early warning systems and special mechanisms for providing national resilience, determining the limits of expedient decentralization in national security, developing adaptive management, and mechanisms of public-private partnership and international cooperation in national resilience should be scientifically and practically resolved.

* * *

The author is sincerely grateful for the support of this new research direction and assistance in elaborating this monograph to the leadership of the National Institute for Strategic Studies, including *Volodymyr Horbulin*, Doctor of Technical Sciences, Professor, Academician of the National Academy of Sciences of Ukraine, Director of the National Institute for Strategic Studies in 2014 – 2018 and *Oleksandr Lytvynenko*, Doctor of Political Sciences, Professor, Director of the NISS in 2019 – 2021.

The author is also deeply grateful to the reviewers *Dmytro Dubov*, Doctor of Political Sciences, Senior Research Fellow; *Oleksandr Korniyevsky*, Doctor of Political Sciences, Professor, Honored Worker of Science and Technology of Ukraine; and *Volodymyr Smolianyuk*, Doctor of Political Sciences, Professor for constructive recommendations and assistance in preparing the manuscript, as well as to *Andriy Smenkovsky*, the Deputy Director and Head of the Center for Security Studies, and employees of NISS scientific departments for their interest in this research, friendly feedback and meaningful remarks, which contributed to improving the monograph.

The author expresses special gratitude to her family and friends for their support and inspiration, as well as to all the professionals who contributed to the publication of the monograph, especially to her husband, *Pavlo Reznikov*, for the unsurpassed design of the publication.

Chapter 1
THEORETICAL FRAMEWORK OF ENSURING NATIONAL RESILIENCE

In recent years, the term “resilience” has been increasingly used in various fields, so it is important to reveal the essence of this interdisciplinary concept, identify its characteristics and manifestations, and distinguish it from other phenomena. Due to the growing complexity of the global security environment, complex and disappointing forecasts for its development in the coming years and decades, studies of the resilience concept in national security draw special interest. In particular, the application of a systematic approach to forming national resilience and determining its basic principles, criteria, processes, and mechanisms have significant theoretical and practical importance.

1.1. The Concept of Resilience in National Security: Research Approaches to Determining Its Content, Structural Elements, and Practical Application

1.1.1. Research Approaches to Forming the Interdisciplinary Resilience Concept

Scientific research on resilience has been going on for a long time. This research pertains to different scientific branches and objects, and the context implies different definitions of this term and proposes fundamentally different resilience ensuring mechanisms. Initially, this term had become common in technical disciplines as a characteristic of certain physical phenomena and processes (for example, the ability of a material or mechanism to accumulate energy and withstand significant loads without breaks and damage). Later, it began to be used in psychology (as one of the individual’s properties helping not to change behavior under the adverse influence or trauma), ecology (as an ecosystems' ability to recover from disasters), and social relations.

The resilience concept is multifaceted, used in different areas, and has different shades of meaning. For example, terms: "polymer resilience," "resilience of a building," "human psychological resilience," "urban infrastructure resilience to natural disasters," "resilience of society to terrorist threats," and "computer system resilience to hacker attacks" are well-known to many people. The "resilience" concept is decisive in each phrase even though it is associated with completely different processes not connected with each other at first glance. However, an in-depth analysis reveals common features of all these cases.

Many researchers, including Martin-Breen and Anderies (2011), Walsh- Dilley and Wolford (2015), Walker and Cooper (2011), Norris, Stevens, Pfefferbaum, Wyche and Pfefferbaum (2008), and others have focused on the diversity of meanings and the transformation of the resilience concept. Their works consider the term "resilience" as a direct research object rather than as a knowledge domain. This implies certain limitations of their research. The authors note that, despite the high popularity of relevant research, there is currently no single definition of "resilience" in the world.

In studying how to define social resilience, Community and Regional Resilience Institute (2013) researchers have concluded that it is hard to choose one ideal definition of resilience among their variety. Each of them has its own significance allowing it to make significant contributions both in the development of various knowledge domains and in interdisciplinary resilience studies. Community and Regional Resilience Institute (2013) experts argue that it is important for this concept definition to reflect the way it is used.

It should be noted that it is not enough to merely semantically analyze the term "resilience" even with modern technologies, including big data, to understand the meaning of this concept for a particular sphere, and even more so to shape systemic measures and policies. In view of this, it is essential to conduct a comprehensive study and discover patterns and links that link resilience with certain characteristics and processes, as well as other concepts in a particular field. That is, *it is necessary to determine the general characteristics of the resilience concept and its manifestations in the field under study*.

While analyzing various research approaches to the definition of "resilience," we can conclude that the following characteristics are fundamental to understanding and further conceptualizing it:

- the field of study;
- the object for which resilience is considered;
- external factors/influences which the object must be resilient to;
- the aim of achieving resilience by a particular object;
- parties interested in the relevant result;
- actors or factors able to influence the achievement of such a result.

Based on the analysis of the above-mentioned studies and thematic glossaries on resilience, developed by a range of research centers (including the Stockholm Resilience Centre (n.d.), the Resilience Alliance (n.d.b), the Disaster Recovery Institute (n.d.), and other authors, we can conclude that in its *generalized form, the "resilience" concept characterizes how an object responds to certain external stimuli and can adapt to their impact without significant loss of its functionality.* The studies have discovered that the resilience concept is ambiguous and tailored when used in different fields, and practices of its implementation are controversial.

Martin-Breen and Anderies (2011) argue that the widespread use of the term "resilience" has not led to the unification of the resilience concept in the areas where it is used, and different researchers use different methods, methodologies, and databases in their relevant works.

Other scholars, such as Walsh-Dilley and Wolford (2015), argue that the existing definitions of "resilience," their conceptualization, and practical implementation are not objective and are based on different assumptions. Such terminological "blurring" causes concern, as it allows us to interpret and apply the resilience concept in a rather inaccurate way. This makes it difficult to assess the concept's impact on development processes. At the same time, the wide scope of research provides an opportunity to rethink what is really important for the development as a complex dynamic process. Walsh-Dilley and Wolford (2015) argue that examination of the resilience concept enables complex thinking, goes beyond the dominant knowledge paradigms, and opens new opportunities for discussion and elaboration of new knowledge inside and outside the traditional disciplinary discourses.

Walker and Cooper (2011) associate the spread of the resilience concept in various fields with the development of systems theory and the introduction of innovative ideas both in theory and in practice. Concurring with the conclusion of these authors, it should be remembered that C. Holling gave significant impetus to the development of resilience studies. Holling (1973) proposed new conceptual approaches in environmental research based on the complex systems theory. The scientist pioneered in defining the "environmental resilience" concept and its formation principles. Holling (1973) also discovered peculiarities of resilience-based management, which shifted the emphasis from anticipating future events as a key crisis management task to building a system capable of adapting to such events, in whatever unpredictable forms they may occur.

Later, these conceptual approaches expanded to the sphere of social and economic relations, and in the 1990s, under C. Holling's initiative, the Resilience Alliance was formed. Later, this organization, which included leading environmental scientists, merged with the Stockholm Resilience Center and expanded its research into sustainable development while trying to reconcile social, economic, and biosphere issues.

It should be noted that in the field of social studies, the resilience concept is based on the general systems theory, including regularities of complex systems formation and functioning. The common features in forming resilience of complex systems of different nature were defined by Holling (1973) through the concept of the system's internal "capital" which "absorbs" external impacts and allows positive systemic changes while retaining the system's structure and basic functions. In addition, scientists distinguished between "resilience" and "stability" concepts, understanding system stability as its ability to return to equilibrium after a temporary disturbance.

Gradually, the outlines of the *interdisciplinary resilience concept and a new approach to resilience thinking* began to emerge. T. Abel, W. Adger, C. Barrett, F. Berkes, M. Biggs, E. Boyd, K. Brown, F. Brand, W. Brock, W. Galas, K. Jacks, J. Ebbesson, K. Eckerberg, A. Duit, S. Carpenter, J. Colding, M. Constas, T. Crane, C. Curtin, C. Lyon, K. Magis, M. Mitchell, D. Nelson, E. van Ness, A. Norström, O. Olsson, J. Parker, S. Polasky, S. Robinson, J. Rockström, H. Ross, J. Stepp, T. Hughes, C. Folke, R. DeFries, M. Schlüter, and M. Shoon contributed to this field of research. The resilience concept has gradually become an integral part of sustainability science.

According to Folke (2016), resilience is the capacity of a system to absorb disruptions and reorganize itself during the change to retain its function, structure, and feedback, and, therefore, identity. In other words, it is the ability to withstand the impact of change and continue to live and develop, even if the environment has changed. At the same time, the scientist noted that resilience thinking was aimed at studying the resilience of socio-ecological systems, their endurance, adaptability, and ability to transform. According to Folke (2016), resilience thinking is "about how periods of gradual changes interact with abrupt changes, and the capacity of people, communities, societies, cultures to adapt or even transform into new development pathways in the face of dynamic change" and "… how to navigate the journey in relation to diverse pathways, and thresholds and tipping points between them." At that, purposeful human actions are important, because, within the resilience concept, adaptation refers to measures that support system development on the current trajectory, while transformation refers to transferring the development to other new pathways or even creating such pathways. According to C. Folke (2016), it is this that explains the dynamic and promising nature of the concept.

In accordance with the definition of resilience published in the Handbook by United Nations International Strategy for Disaster Reduction [UNISDR] (2009), resilience means "the ability of a system, community, or society exposed to hazards to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions." The key is the ability to "resile from" or "spring back from" a shock. UNISDR (2009) noted that the "resilience of a community in respect to potential hazard events is determined by the degree to which the community has the necessary resources and is capable of organizing itself both prior to and during times of need."

Proposing an alternative research approach, Hodicky et al. (2020), argue that resilience is mostly about the measurement of capacity, and its concept is uncertain.

Summarizing the resilience discourse, Carpenter and Brock (2008) note that resilience is a broad, multifaceted, and loosely organized cluster of concepts, each one related to some aspect of the interplay of transformation and persistence. Thus, resilience does not come down to a single theory or hypothesis. According to the scholars, resilience is a constellation of ideas, testable through various practices.

The analysis of various research approaches to the content of the interdisciplinary resilience concept allows us to conclude that they revolve around the ability of complex systems to respond to adverse impacts in a way that allows them not to lose their functionality and ability to develop. As resilience manifestations in different fields may vary, the aim of the monograph makes it necessary to analyze how the resilience concept is implemented in the field of national security.

1.1.2. The Evolvement of Security Studies

Resilience as a security category came to be considered somewhat later than in other fields. This is due to the fact that national security studies has been formed only in the second half of the 20th century, and the combination and mutual enrichment of national security research and resilience studies occurred at the beginning of the 21st century.

The term "national security" became widely used at the beginning of the 20th century when the role of the state in the system of social relations, ways of exercising power, and protection of national interests was conceived. The development of the international relations theory in the 2nd half of the 20th century contributed to the intensification of national security studies. If national security was initially considered primarily in the classical realism international relations paradigm, then later national security issues were studied within other paradigms: liberalism, the English school, strategic studies, critical theory, peace studies, etc. Eventually, a separate research direction – security studies – emerged.

In the 2nd half of the 20th – early 21st century, conceptual approaches to national security, as well as the security concept itself, have significantly changed. After World War II, the traditional approach to defining security within the political realism paradigm dominated, in which a state played the main role in providing security, an external war was considered a key threat, interstate conflicts were considered highly probable, and force was to be a key to resolve them. Besides, state security was practically synonymous with personal security, as it was considered an indispensable condition for the well-being of citizens. According to Jones (1999), this approach was too static and limited.

The events of the last decades of the 20th century, in particular the end of the Cold War and the USSR collapse, did not fit into it. Meanwhile, the scholar notes that such radical changes took place exclusively by peaceful means.

After the events of the above-mentioned period, as Thompson (1982) predicted, not "détente," but rapid and unpredictable changes, disruption of ties between states, and acute intra-state conflicts, resembling "mapless movement" should have happened.

Under the new circumstances, the narrowed (traditional) approach to the definition of national security, which focused on the military component and had a state-centric character, needed to be revised. The change in the security environment has highlighted a wider range of threats and dangers than military ones, and new non-state actors in this field have become more active. For example, the traditional research approach has overlooked the security implications of rapid technological change, including in transport, energy, and information.

Under such conditions, the securitization theory, proposed by B. Buzan, O. Weaver, and other representatives of the Copenhagen School, became popular. According to Buzan and Weaver (1998) the new research approach has expanded the security concept to include political, economic, social, and environmental components in addition to the military one. At the same time, the scientists recognized the key role of the state in providing national security.

Ullmann (1983) stressed that interpreting the term "national security" only in the context of countering military threats diverts attention from non- military dangers and does not take into account many aspects of vital human interests. Based on the conclusion that it is impossible to achieve world peace if people are not safe in their daily lives, United Nations Development Programme

(1994) formulated in the Human Development Report a new scientific *"priority of human security" concept* and its components: economic security, food security, health security, environmental security, personal security, community security, and political security.

In general, in the early 1990s, many studies explored the role of security actors other than the state including citizens, society, ethnic groups, and religious organizations. The scientific and expert community, including Booth (1991), began to raise the issue of "emancipation of security" as its release from restrictions. As we can see, the changes in the national security concept interpretation proposed by researchers during this period were aimed at making the national security system more flexible.

The security issue has become more addressed not only at the national level but also at other – regional and global – levels. After the globalization concept appeared, discussions about the role of nation-states in the context of strengthening their ties and mutual influence, the emerging players in the international arena, and the formation of global networks have intensified. The changes that have taken place in the world under the influence of globalization have not made the world safer. According to Held and McGrew (1998), an emerging complex system of interstate political and economic ties left only a little difference between national security strategies and international security strategies for many states. They also argue that globalization is driving the transition from a state-centric policy to a new comprehensive form of multi- layered global governance in the field of security. Although countries with different potentials and development levels have benefited differently from globalization, there is a general tendency of reducing the ability of nation-states to ensure national security due to a lack of their institutional capacities. This has put the need to transform political systems at both national and international levels on the agenda in order to bring them more in line with the new global development conditions.

We should also pay attention to the discourse in which nation-states (especially global leaders) have expanded their understanding of security beyond the principle of protecting and promoting national interests in favor of interventions (external interventions) in cases when human rights need protection, which was enabled in light of the emerging "global community" theory and the development of the concept of prioritizing human security. This, in particular, was pointed out by Chandler (2012) in his analysis of the paradigm shift in security studies.

However, the concept of "strong" states being responsible for global security and their right to interfere in the internal affairs of other states to protect basic human rights proved to be quite problematic in practice and created fundamental contradictions between this right and the sovereign rights of independent states.

Furthermore, such global security measures required adequate resources and became quite burdensome for the national economies of the "strong" states.

Changes that have begun in the global security environment, emerging new and exacerbating traditional threats have mainstreamed questions about the flaws of the existing security systems and their inconsistency with new circumstances.

This has led to an assumption that national security systems needed to acquire new characteristics, which would allow states to independently counter threats and hazards of any nature and origin. Within this approach, the role of "strong" states had to change from providing direct protection to the "weak" states to helping them to develop the ability to adapt to changes in the security environment and to counter threats on their own. In fact, a question about state resilience-building arose.

In general, in addition to the above-mentioned, the following works of famous scholars also contributed to shaping and developing a separate scientific direction of security studies: M. Barnett, T. Balzacq, D. Bezvik, A. Bellamy, K. Buza, T. Weiss, P. Williams, J. Duffield, H. Dexter, D. Joseph, B. Evans, J.

Reid, S. Tang, J. Hertz, J. Hoogensen Gjørv, L. Friedman, M. Foucault, and D. Chandler. These issues were also studied by the following Ukrainian scientists: O. Belov, V. Gorbulin, D. Dubov, B. Kaczynski, O. Kornievsky, V. Kosevtsov, N. Nyzhnyk, O. Lytvynenko, G. Sytnyk, and V. Smolyanyuk.

1.1.3. Features of Using the Resilience Concept in National Security

Due to evolving conceptual approaches to national security, developing systems theory, and forming resilience thinking the resilience concept expanded to security studies and the notion of *"national resilience"* has emerged. Further insights and streamlining of the relevant knowledge enabled the formation of an independent concept of national resilience. Among the researchers of this concept are J. M. Anderies, P. Bourbeau, J. Joseph, B. Evans, C. Zebrowski, M. D. Cavelti, M. Kaufmann, K. S. Kristensen, M. Cooper, P. Martin-Breen, G. Laskonjarias, V. Proag, J. Reid, J. Walker, K. Fieder, and D. Chandler.

Studying the emergence and development of the national resilience concept, Walker and Cooper (2011) point out that over the past decade, the topic of resilience has become widespread as an operational strategy for emergency preparedness, crisis response, and national security. Lasconjarias (2017) argues that building national resilience has become a crucial task for states, as it allows them to prepare for countering threats of a new type, which manifested after the hybrid aggression of the Russian Federation against Ukraine in 2014. According to Fjäder (2014), the national resilience concept has emerged in the national security agenda from the expanding range of new threats due to growing global interdependence and uncertainty. The scientist notes that under such conditions, providing security by nation-states is becoming an extremely difficult task and requires new approaches, including the development of national security strategies with due account for national resilience principles.

At the same time, not all researchers interpret the national resilience concept in the same way. Joseph (2013) and Zebrowski (2013) consider national resilience as a special form of governance from the perspective of neoliberal ideas of reducing the role of the state. Critics of the national resilience concept, including Evans and Reid (2015), point to its depressive nature, as it views the real world solely through the prism of threats and imminent catastrophes, thus creating constant anxiety and danger as a "new reality" framework. Besides, Evans and Reid (2015) conclude that the ideology of national resilience changes the public administration principles and political rules, shifting much of the responsibility to the population, which must prepare to live under constant threats.

The study by the Community and Regional Resilience Institute (2013), which analyzes the terms used in social resilience, identifies key classes in the interpretation of the resilience concept in national security depending on the ways of providing resilience, namely:

- resilience as a certain *ability* of an object – a static approach; or as a *process* of achieving a determined result – a dynamic approach;
- strengthening resilience through the object's *adaptation* to cope with adversity or to prevent or *resist* its impact;
- resilience in the context of possible changes (*trajectory*): the first approach proposes to consider an object which survives adversity as resilient, (if it does not – as not resilient), and the second proposes to consider an object that was able to regain its functionality after the crisis also as resilient;
- resilience in the context of predictability of adversities (*predictability*): the first approach considers resilience as the ability to anticipate a threat and prepare for possible adverse impacts in advance, and the second approach considers resilience as the ability to respond to threats effectively;

- temporal or permanent nature of resilience as an immediate crisis response or a dynamic process of preparation to, response to, and recovery from crisis.

As for complex systems resilience, having analyzed numerous studies (Ashby, 1960; Bertalanffy, 1968; Chandler, 2012; Folke 2016; Gunderson & Holling, 2001; Holling, 1973; Holling, 2001), we can identify the following main differences in defining the essence of this phenomenon, namely due to its ability to:

- absorb disruptive impacts and violations of integrity to maintain or regain equilibrium;
- quickly regain equilibrium after environment changes or adversities;
- effectively counter disruptive impacts and other adversities by adapting to their action, including through transition to a new equilibrium.

These differences determine different approaches to ensuring resilience in national security and forming relevant public policy and mechanisms.

In the modern world, there are more and more security challenges and threats to humans, society, and the state. They become more complex and almost impossible to prevent or overcome. Countering such threats usually requires an integrated approach and joint efforts of different national security actors. The concept of resilience should be introduced in national security because of the need for a timely and effective response to a wide range of threats and crises to prevent destructive processes in the state and society caused by their vulnerabilities or inability of the state to perform critical functions.

The implementation of the relevant set of tasks becomes especially crucial in the context of countering hybrid threats. They feature coordinated simultaneous use of a wide range of traditional and non-traditional methods and means of struggle in various fields and active involvement of non-state actors.

Combined methods of influence cause a synergistic effect. Besides, hybrid threats are often covert or disguised as other processes within the legal field.

Therefore, such actions are often difficult to identify as threats, especially at an early stage. A hybrid war aims not to establish control over a certain territory, but to destabilize the state and society under aggression and to weaken their ability to protect national interests and values. The continuing aggression of the Russian Federation against Ukraine, which began in 2014, is carried out using this very technology (Horbulin et al., 2017).

A response to hybrid threats, which are mostly long-term and create a situation of uncertainty, must also be comprehensive. In turn, this requires the national security system to be upgraded. However, building capabilities of security and defense forces alone is clearly not enough to strengthen national resilience. In this context, the application of the resilience concept to the field of national security helps form a state strategy that allows the state to overcome threats, crises, and other hazards of any origin and provides acceptable conditions for the state and society to function even in crises. The relevant mechanisms have to be developed and implemented to formulate and implement state policy in national security and resilience.

As Cavelti, Kaufmann, and Kristensen (2015) note, considering the interdisciplinary nature of the resilience concept, it aims to offer universal mechanisms for resilience, survivability, and security that would equally satisfy individuals, society, ecosystems, and technical systems.

National resilience studies is a quite new and promising field for many countries, including Ukraine. National resilience as an effective state and society development vector in conditions of uncertainty should be strengthened with due account for national interests and development prospects. In this regard, the practical implementation of the resilience principles and mechanisms in various fields requires an understanding of the basic theoretical regularities and conceptual approaches in this area, as well as the application of relevant methodology. Otherwise, it is possible to encounter the inconsistency of practical results with the planned tasks and declared intentions.

Now we can see that recommendations in national resilience provided by some Ukrainian and foreign advisors are sometimes divergent and fragmentary. This results from different interpretations of the national resilience concept and differences in conceptual approaches to its formation offered by representatives of the scientific and expert community. Due to the specific features of different disciplines and areas of activity some terminological confusion and substitution of concepts often emerge during the practical implementation of the resilience concept. For example, the following terms are sometimes used as synonyms for "resilience" in the security sphere: "power," "steadfastness," "reliability," "survivability," "security," "stability," "immutability" and even "stagnation" (as resistance to change). These terms have close meanings with certain semantic nuances and characterize different aspects of certain processes or states of a particular object. But they are not completely identical.

For example, the definition "state power" refers primarily to state resource potential in a broad sense (as a set of material and spiritual capabilities available to the state and used to achieve its geopolitical goals (Kachynskyi, 2015)). The concept of "survivability" characterizes a system's ability to remain within safe limits of balanced functioning (Gigch, 1981b). This term is used primarily to describe biological organisms, as well as technical systems (e.g., energy, transport). The term "reliability" can be used as a synonym for resilience regarding technical systems. To characterize the balance in the economy, social relations, and ecology, the terms "stability" and "sustainable development" are usually used. Sukhodolya (2018) draws attention to the peculiarities when such terms are used in energy security, and Boyko (2014) – in the economic sphere. In the medical sphere, the term of resilience in the sense of "resistance" to medicines or treatment (meaning a lack of response or changes in the patient's health) is widespread in Ukrainian society (due to the use of the same word in Ukrainian). In the security sphere, the term "resistance" can be interpreted as opposition to the enemy, including through sabotage, subversion, and guerrilla movement. This term also differs from the definition “resilience” which has broader sense and characterizes mainly the dynamic processes linked with change.

Therefore, given the variety of above-described definitions, we can emphasize the need to elaborate a common terminology in the national resilience field. It should be noted that there are different approaches to the definition of “national resilience” in the scientific community. In most states and international organizations, which have recently paid considerable attention to resilience building, appropriate glossaries have been created and are used to eliminate confusion and ambiguity in the elaboration of governing documents. There are both thesauri providing interpretations and definitions of all terms and concepts used in this field, and special glossaries of individual reports, articles, documents, etc. The following references deserve attention:

- International Glossary for Resilience (Disaster Recovery Institute, n.d.);
- Security and Resilience Vocabulary of the International Organization for Standardization (ISO, 2021);
- Australian Disaster Resilience Glossary (Australian Disaster Resilience Knowledge Hub, n.d.);
- Glossary: Resilience. Evidence on Demand (UK Government, 2016) as part of a series of inter-related resources synthesizing knowledge on resilience;
- Glossary English from the report: AR5 Climate change 2014: mitigation of climate change (Allwood, Bosetti, Dubash, Gómez-Echeverri & Stechow, 2014) as part of the UN Intergovernmental Panel on Climate Change reports[1];
- Online glossary of the UNISDR (United Nations Office for Disaster Risk Reduction, n.d.), established in accordance with the recommendations of the report of the intergovernmental expert working group on terminology

[1] The Panel was established in 1988 by the World Meteorological Organization in collaboration with the UN Environment Programme to assess scientific information on climate change and formulate realistic strategies for responding to the consequences; it prepares reports used in the work of the parties to the UN Framework Convention on Climate Change.

relating to disaster risk reduction, adopted by the UN General Assembly on February 2, 2017;

- Glossary of Humanitarian Terms (ReliefWeb, 2008);
- Glossary of basic terminology on disaster risk reduction (UNESCO, 2010);
- Glossary of the FEMA, US Department of Homeland Security (Federal Emergency Management Agency, n.d.a);
- Glossary of Key Terms in Evaluation and Results Based Management (OECD, 2002).

In 2017, the International Organization for Standardization (ISO) included the “organizational resilience” concept as the ability of an organization to absorb and adapt to a changing environment in the “Security and Resilience” section of the Standards Catalog (ISO, 2017a).

A team of scholars from Israel and Canada (Canetti, Waismel-Manor, Cohen & Rapaport, 2013) conducted a survey among students at a number of universities in Israel and the United States to determine their perceptions of the definition “national resilience.” According to Canetti et al. (2013), respondents’ understanding of this term was influenced both by their individual perception of major threats to national security and by a number of national peculiarities and political-psychological aspects (including trust in national institutions, patriotism, optimism, social cohesion, historical experience, and cultural differences).

There was little difference in “national resilience” definitions made by Americans and Israelis: the generalized American version was more abstract, while the Israeli version was more detailed (Canetti et al., 2013). In general, due to results of this survey, the essence of this concept was defined as the ability of a nation to successfully overcome threats (e.g., terrorism, corruption, and poverty) while keeping social values intact.

Generally agreeing with the conclusions of the above-mentioned researchers regarding the content of the “national resilience” notion, we should add that it focuses on such definitions as a nation, threats, and social values. It also allows for the application of an integrated approach in terms of counteracting a wide range of threats, crises, and other hazards; and it identifies certain functional characteristics (in particular, safeguarding social values).

However, such a characteristic of national resilience as “the ability to successfully overcome threats,” mentioned by Canetti et al. (2013), is too generalized and does not reflect all the inherent features of the “national resilience” definition. First of all, it is about adaptability which allows the state and society to adapt to the constant influence of threats and rapid changes in the security environment, function continuously during crises, and recover quickly from destructive effects of any kind of threats and adversities to optimal equilibrium under the determined conditions (Reznikova, 2018d).

Given the main provisions of the resilience concept in national security, it can be argued that the adaptability of the state and society means not passively executing the will of a stronger party of relations at the expense of national interests, but a purposeful search for new formats of interaction and mechanisms for the protection of national values and interests, which could continue to function effectively under long-term or imminent threats and hazards.

Analyzing the various definitions of “resilience” and taking into account the alternative conceptual approaches outlined in the above-mentioned studies, we can reveal key features of the “national resilience” definition that distinguish it from other terms and form the basis of a national resilience concept.

First of all, the issue of national resilience concerns security and development of *state* and *society*. *Threats* to national security, *challenges*, and *crises* are also one of the defining characteristics of the national resilience concept. In turn, the need to *respond* to threats and crises requires appropriate actors, capabilities, and mechanisms capable of adapting to change and effectively overcoming hazards and crises in various spheres. The need to combine two opposite processes (that is *movement* and *immutability*) within this concept should also be considered. It means that some systemic characteristics and processes in the state and society must remain unchanged while others may significantly change, provided the integrity and functionality of the main objects remain intact. Here, the key constants may be, in particular: the need to preserve national values and protect national interests, providing the continuity of the essential services, which the state provides to the population, as well as acceptable living conditions for society and the state. Dynamics is determined by the need to timely and effectively respond to rapid changes in the security environment, new challenges and threats, and the ability to adapt to their permanent or long-term influence. According to this paradigm, the *aim* of ensuring national resilience can be determined.

So, the meaning of the “national resilience” definition can be described as follows: **national resilience** is the ability of the state and society to effectively counter threats of any origin and nature, adapt to rapid changes in the security environment, function continuously, including during crises, and quickly recover after crises to the optimal equilibrium under the reasonable conditions (Reznikova & Voytovskyi, 2021).

That is, the state, society, organizations, institutions, and other objects and parties, as well as certain technical, technological, organizational, and operational systems functioning within the particular state, should acquire a certain *set of qualities* necessary for their secure existence, sustainable functioning, and development in conditions of uncertainty and increased risks, as well as the ability to quickly recover after crises. Determining the limits of transformations that various complex systems can undergo in adapting to adversities while maintaining their functionality, development capability, elemental composition integrity, and system links is currently one of the most controversial issues and requires further research.

In order to avoid terminological confusion, it should be noted that in this case the definition of "national resilience" is used not in the context of preserving integrity and development of a particular ethnic group, but in a broader sense, related to the existence of collective identity and nation-wide political organization. According to many modern scholars,[2] including Rozumnyi, Stepykom, and Yablonskyi (2012), the phenomenon of the nation is complex and multifaceted, it characterizes a certain socio-cultural and historical community, which should not be considered only from the perspective of ethnic characteristics. Rozumnyi (2016) notes that nation-building processes are complex, multidimensional, and multivariate. The scholar argues that currently the concepts of civil society and political nation are equally present in the public consciousness as landmarks of national development and socio-political transformations.

That is, in the above-mentioned "national resilience" definition, the word "national" means belonging not to a particular ethnic group, but to a specific nation state. At the same time, it reflects not only the processes around the state as a political institution and its ability to overcome threats, but also covers a wider range of social relations and objects.

Summarizing the above, as well as taking into account the recommendations of the Resilience Alliance (2010) for assessing complex systems resilience, we can identify key issues, systemic elements, and links that represent the quintessence of the resilience concept in national security (*Table 1.1*).

[2] Українська політична нація: проблеми становлення : зб. наук. ст. / за ред. М. М. Розумного (заг. ред.), М. Т. Степика, В. М. Яблонського. Київ : НІСД, 2012. 384 с. – Ukrainian Political Nation: Problems of Formation / collection of scientific articles edited by M. Rozumny, M. Stepyk, and V. Yablonski – Kyiv, NISS, 2012.

Table 1.1

Key Characteristics of the National Resilience Concept

Key issues of national resilience	Semantic content	System elements and links
Resilience of what?	Object of resilience	State and society
Resilience to what?	Adversities (stimuli)	Threats, crises, or impacts to which the object must be resilient
What for?	Aim and level of resilience	Adapting to the changing and uncertain security environment while preserving national values and protecting national interests
Whom for?	Parties interested in obtaining the relevant result	Public and local authorities, civil society, scientific institutions, communities, business, and the population that become better protected
Who will do it?	Parties able to ensure achievement of the relevant result	Public and local authorities, civil society, scientific institutions, communities, business, and the population that take the determined measures on strengthening security and resilience of the state and society

Source: developed by the author.

Given the above considerations on the content and key characteristics of the national resilience concept, we can argue that this phenomenon has features of complex systems. We are talking about the basic system elements and their links: objects, subjects, aim, critical parameters, functions, management principles, etc. A set of relevant elements and links makes a *national resilience system*. This conclusion is important not only to understand the specifics of the application of the interdisciplinary resilience concept in national security, but also to develop specific mechanisms and practical recommendations to formulate the relevant public policy.

In light of the above, using a systems approach, it is expedient to analyze features of providing national resilience and formation and functioning of the relevant system, to identify common features and differences that make the national resilience ensuring system different from the national security ensuring system, and to analyze possible interactions between the two systems.

1.2. National Resilience Ensuring System: Its Essence and Main Characteristics

1.2.1. The Essence of the National Resilience Ensuring System

Based on the systems theory, in particular the studies of Ackoff (1971), Ashby (1960), Bertalanffy (1968), Bogdanov (2003), Parsons (1977), Prigozhyn and Stengers (1986), Setrov (1988), and Scott (1961), it can be argued that the national resilience system, like any other complex system, is a set of objects, subjects, aims, critical parameters, functions, and management principles. Combined according to certain rules, they must be focused on a certain result of system functioning, which will differ from (usually overwhelm) the results that can be produced by its individual elements or other systems.

While applying a systems approach to the national resilience system analysis, the following basic regularities should be considered:

- social phenomena should be considered as systems (Bertalanffy, 1968);
- systems have structures that are a stable unity of elements, their links and system integrity (Ovchinnikov, 1969);
- a system is a set of interrelated variables (Ashby, 1960; Scott, 1961);
- a system is characterized by system parameters – attributes by which it can be identified and classified (Uyemov, 1969);
- complex systems contain simpler systems (Sachkov, 1969);
- complex systems are open, constantly interact with external environment, function purposefully, are able to solve different groups of tasks, and have different levels of structural organization (Sachkov, 1969; Ashby, 1960).

We will also take into account other formation and operation regularities of complex systems during further analysis.

As in the case of the national security system, the national resilience system needs a mechanism to ensure its functioning and development and enable the interaction of all its components so that the system will begin to produce the expected result. Its key purpose is to perform certain actions aimed to achieve the determined goal. The national resilience ensuring system is a holistic and structured mechanism with closely linked elements, including a common mission and aim. A break of links between the elements of this system can lead to its damage or destruction. The integrity and balance are influenced by feedforwards and feedbacks between its elements, the nature of interaction with other systems, and influences from the internal and external security environment, etc.

Therefore, taking into account the previously proposed definition of national resilience and the content of the relevant concept, **the national resilience ensuring system** can be defined as a comprehensive mechanism of interaction between public and local authorities, institutions, enterprises, NGOs, and people, as well as targeted actions, methods, factors and mechanisms that safeguard the security and continuous functioning of key spheres of the society and state before, during, and after crises, including through adaptation to threats and rapid changes in the security environment (Reznikova & Voytovskyi, 2021).

The main **stimuli** (adversities) to which the national resilience ensuring system must respond are threats of any nature and origin, crises, and other hazards. As Rapoport (1969) found out, an input together with a certain system state determines the output and a possible system transition from its initial state to another. At the same time, while stimuli (inputs) can affect various system elements, they, first of all, influence objects that largely determine the system outlines and must gain the determined qualities according to the established aim (Rapoport, 1969). It means that various threats and crises can adversely affect national resilience objects in different ways and intensities, disrupting both their elements and system links. However, the functional national resilience ensuring system is devoted to preserving the integrity of both objects and system links, giving them the ability to absorb such influences, counteract them, adapt to impacts without significant loss of functionality, recover, and develop after crises.

1.2.2. Characteristics of Objects and Actors in the National Resilience Ensuring System

The key **objects** of the national resilience ensuring system are the *state* and *society*, which may experience destructive impacts (threats, crises, and other hazards). They themselves and their components must have the above- mentioned qualities necessary for a sufficiently safe existence, functioning, and development in conditions of uncertainty and increased risks.

In general, any things (metals, structures, etc.), social and technical systems (political, economic, energy, informational, infrastructural, etc.), people, or organizations may become objects of resilience. As complex systems, they have resilience potential which can be enhanced. The state and society as key national resilience objects are also complex systems. Their elements and system links may be affected differently by different threats, therefore the mechanisms for strengthening the resilience of the state and society may also differ. To determine what specific mechanisms and practices should be used to enhance the resilience of individual components of the state and society, it is necessary to apply the decomposition method to these objects. At the same time, it is important to take general systemic characteristics of key objects, their internal links, and interaction with other elements of national resilience ensuring system into account. In this context, the following conclusions about complex systems' features made by Ovchinnikov (1969) are noteworthy: one object can be represented as different systems unity; during the study, an object as certain integrity may disappear from the scene shifting attention to the subject of the study determined by the conditions of the formulated task.

As we know from the systems theory, resilience is one of the conditions for the existence of any system. So, the question may arise: why do we need a national resilience ensuring system at all, if its main objects are a priori resilient?

However, the resilience of a complex system is not absolute and constant. In response to environmental changes, systems seek to restore their initial state of stability or reach this state at a new level. This can be reached in different ways. The variability of complex systems' adaptability and features of adaptive behavior was pointed out, in particular, by Ashby (1960).

There is also the phenomenon of systemic contradictions, which was studied, in particular, by A. Bogdanov and E. Vinogray. According to Bogdanov (2003), a system develops towards the most stable relations, both internal and between the system and its environment. A contradiction may become apparent in the fact that stable links do not always determine the system development vector but may cause a certain equilibrium to preserve. One way to resolve system contradictions and increase system resilience is to make additional links. As Vinogray (1989) notes, the more precisely the system elements complement each other functionally, the higher the system focuses its actions in a certain direction. This is the basis of the principle of function-added relations in the system.

Given that the modern security environment is becoming more aggressive for the state and society, and adversities are more destructive, it seems reasonable *to create an additional comprehensive mechanism aimed to strengthen the resilience of these objects in the perspective of their further existence, security, and development*.

As complex systems, the state and society also consist of various components, including subsystems.

Certain measures may be taken to strengthen some subsystems or make them more resilient. Such *subsystems* may be classified according to various indicators, in particular, according to the:

1) *sphere of social relations* where they manifest: economic, political, social, and spiritual;
2) *organization level*: national, regional, sectorial, group, and object;
3) *sphere of activity*: economic, environmental, technical, infrastructural, governance, and security.

Depending on the object, scientists often distinguish different subtypes of national resilience: social, technological, and organizational.

Resilience objects may group according to certain features. Taking into account that stimulus's impact is one of the determinants of national resilience system objects, scholars often distinguish areas and sectors of providing national resilience based on the nature or sources of threats.

In order to assess national resilience, a report, prepared for the World Economic Forum [WEF] (2013), suggested singling out the following national subsystems: economic; environmental; governance; infrastructure; and social.

Based on this study, Donno (2017) identified five main areas where threats are most likely to occur, and their impacts can be most devastating, namely: economic, technological, societal, geopolitical, and environmental. Accordingly, the researcher proposes to focus on the resilience of the following sectors: government; agriculture and food; energy and nuclear; water and wastewater; transportation; defense; health; communication and information technology (IT); financial; education; chemical; retail; manufacturing; social services; and tourism.

According to another researcher on this issue, Proag (2014), system resilience matters for a range of the following key sectors: technical, political, organizational, social, legal, economical, ecological, and environmental.

In addition to these scholars, Bourbeau (2013), Rogers (2013), Walklate, McGarry and Mythen (2013) proposed different approaches to the national resilience typology depending on the object or nature of threats.

In general, analyzing numerous scientific publications and existing world practices, we can argue that determining key areas of the national resilience depends on the nature and sources of major national security threats (in terms of their possible manifestations and impacts on different spheres), and the main sectors of resilience development should be determined by processes and activities critical to the sustainable functioning of the state and society.

Therefore, it is expedient to determine the following *key spheres of providing national resilience*: economic; environmental; technological; geopolitical; public relations. The *main resilience-building sectors/directions* can be identified within these spheres, in particular: governance; defense and civil protection; critical infrastructure, including water, food, and energy supply, transport, information infrastructure; healthcare; economy and finance; education; retail; social services; internal affairs and foreign policy (*Table 1.2*).

Table 1.2

Key Sub-Systems

of the National Resilience Ensuring System Depending on Object

Base attribute	Classification
1. Nature and source of threats and crises that adversely impact the objects in terms of their possible manifestations and consequences	*Spheres*: • economic; • environmental; • technological; • geopolitical; • public relations
2. Processes and directions critical to the continuous functioning of the state and society	*Sectors*: • governance; • defense and civil protection; • critical infrastructure, including water, food, and energy supply, transport, information infrastructure; • healthcare; • economy and finance; • education; • retail;

	• social services; • internal affairs; • foreign policy
3. Organizational levels of key objects of ensuring national resilience	*Levels*: • national; • regional; • sectorial; • group; • object; • individual

Source: developed by the author.

It is important to determine key spheres and sectors/directions for providing national resilience in order to select a model, which will become a basis for organizing the national resilience ensuring system in each country. Such models may significantly differ in various countries depending on their national interests or governance peculiarities.

An individual can also be an object under threat. In particular, it is about risks of loss of life, health, or property due to an emergency or illegal actions of others. As long as the adverse impacts on individuals are isolated and not systematic, they do not pose a threat to national security. If they cover many people across the country, individual groups, communities, or society as a whole become objects under threat. To determine specific mechanisms for providing national resilience to various threats, it is important to analyze threats and other adverse impacts and their consequences for various target groups, including individuals. Thus, *characteristic features of national resilience ensuring system objects in terms of the stimuli' impact are the scope of the relevant effect and its relation to the national security status.*

While forming resilience of the state and society (as key objects) and their subsystems, it is important to realize what their elements/characteristics should remain *unchanged* during adaptation to changes in the security environment in order to ensure their integrity and/or ability to perform basic functions, and what elements could be *modified, supplemented, or removed* in order to achieve the determined aim and ensure development in difficult circumstances. So, the national resilience concept combines such processes as *movement* and *immutability*.

Given that an object's resilience is not an absolute value but may change in a certain way, it is necessary to discover how we can influence it, and, in particular, raise the resilience of a particular object to the determined level. This raises a question about the role of actors, methods, factors, and mechanisms for ensuring national resilience.

The main **actors** in the national resilience ensuring system are *public and local authorities, enterprises, institutions, organizations, civil society structures, and citizens that initiate or participate in the national resilience providing processes* (Reznikova & Voytovskyi, 2021). Purposeful activities of these actors enable objects to acquire necessary characteristics, namely: the ability to effectively resist threats of any origin and nature, adapt to rapid changes in the security environment, function continuously (including during crises), and quickly recover after a crisis to the optimal equilibrium under the determined conditions.

One of the distinctive features here is that *objects can transform into actors* in the national resilience system. The point is that a person, organization, society, institution, or state is no more considered a purely passive object of threat but begins to acquire (independently or assisted by other actors) necessary qualities and capabilities to actively resist threats, crises, and their consequences, as well as adapt to new security conditions. In this way objects strengthen their own resilience, using both self-development potential and the capabilities of the national resilience ensuring system. Transforming resilience objects into actors has been studied, in particular, by Cavelti, Kaufmann, and Kristensen (2015).

Chandler (2012) believes that a resilient object (both at the individual and collective level) is never considered passive or insufficiently free but only as an active actor able to achieve self-transformation.

Within the traditional research approach to national security, the state, represented by the authorized state bodies (actors of the national security ensuring system), was entrusted with the main functions of providing the security of citizens, institutions, enterprises, organizations, etc. (objects of the national security ensuring system), including in case of terrorist attacks, natural disasters, and other emergencies. At the same time, citizens, institutions, enterprises, and organizations can independently or in cooperation with others take measures to increase their own security and resilience, turning from passive security objects to active actors in providing national resilience.

The initial response is performed usually at the lowest level, especially when a human is under threat. In an uncertain security environment, strengthening national resilience at all levels, from state to object, is particularly important. At the level of individuals, it is expedient to take measures to increase individual security and resilience (for example, raising awareness of existing and expected threats and hazards, obtaining skills necessary to respond to them, attending self-defense courses, and improving legal and informational awareness) This requires a responsible attitude of citizens to their security.

According to Cavelti, Kaufmann, and Kristensen (2015), in the modern world, the security or insecurity of an object is determined not only by the nature and level of threat but also by its qualities, namely how resilient the object is to adverse impacts and hazards.

Most often, researchers distinguish the following organizational levels of the national resilience ensuring system: state, regional (within the state), local (territorial communities level), and object (organizational resilience). There may also be supranational resilience ensuring systems: regional (interstate) and global. Chandler (2012) pointed out the international nature of resilience in his studies.

1.2.3. System Links in National Resilience

The above considerations about national resilience objects acquiring subjectivity allow us to conclude that *system links and processes of providing national resilience have special nature determined by their proactivity*. It is not only about the ability of objects and actors to promptly and effectively respond to threats and crises, but also about their active influence on the environment to prevent threats, reduce their adverse impacts, create the necessary capabilities, and strengthen system links. Practical implementation of such an approach requires changing the paradigm of thinking in order to form a more active and responsible stance of people for the current and future consequences of their actions or inaction. This, in turn, should be reflected in education at all levels, including in training staff for the national security and defense sector.

By enhancing individual resilience, actors not only increase their chances to overcome or adapt to threats and hazards of different nature and origin but also contribute to national resilience-building in general. For example, if an individual household installs solar panels, wind turbines, and other alternative energy sources, then it will increase its individual resilience to the risks of state/regional power grid disruptions. If all households, enterprises, and organizations take such actions, then we can talk about large-scale measures and strengthening national resilience in certain directions and criteria, because reserve capacity and alternative strategies will be formed. At the same time, increasing organizational resilience and clearly-defined responsibilities in providing national resilience of state and local authorities, communities, organizations, and individuals will foster their preparedness and effectiveness in responding to a wide range of threats. In this context, we can consider national resilience as *a set of resilient objects and resilient actors* (Kaufmann, Cavelty, and Kristensen, 2015; Reznikova, 2018d). Close *links and mutual influences* between objects and actors determine the complex and comprehensive nature of national resilience-building measures which should cover political, economic, social, informational, psychological, and other aspects. Such connections are embodied through purposeful actions, relevant methods, factors, and mechanisms. At the same time, the national resilience ensuring system interacts with the external environment, which includes other systems. Here, new links (which will help develop key objects and the national resilience ensuring system in general) and additional negative impact factors may arise. Interaction of actors and objects is conditioned by a certain purpose and is aimed to achieve such results, as reducing risks of crises and their impacts, continuous functioning of the state and society under any conditions, strengthening the resilience of key objects and their components against internal and external adversities (stimuli), including through strengthening the existing and forming new system links. The diagram of the interaction between key elements of the national resilience ensuring system and the external environment is shown in *Fig. 1.1*.

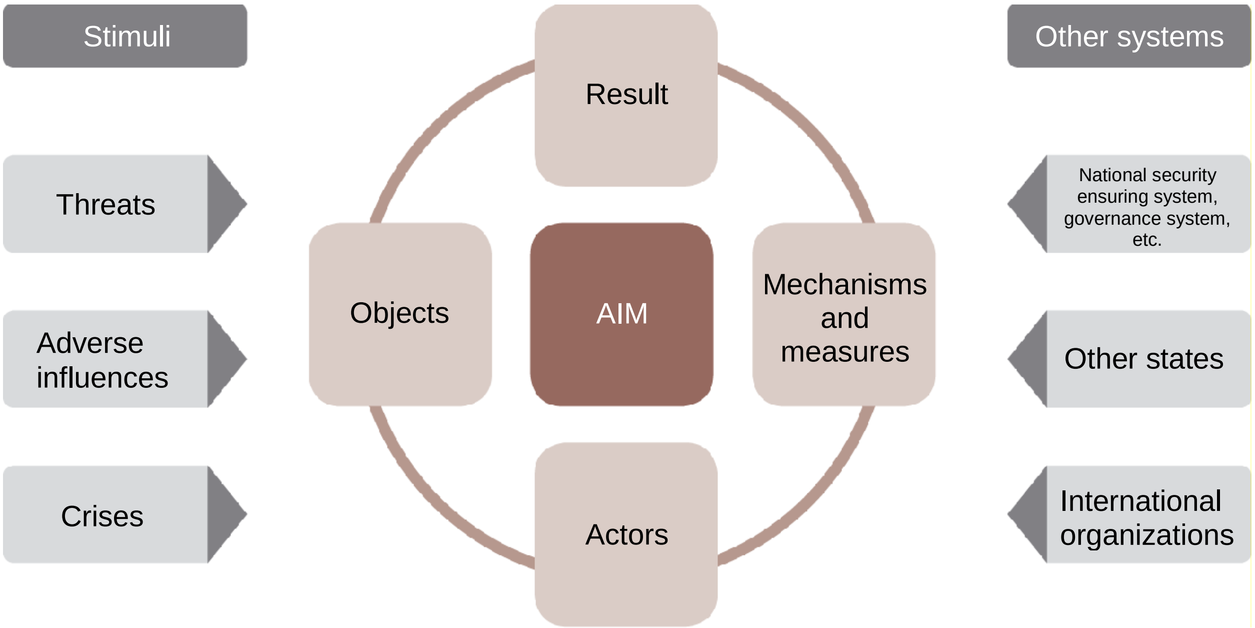


Fig. 1.1. Interaction between the national resilience ensuring system and external environment

Source: developed by the author.

Complex systems’ elements can be other systems that interact with each other in keeping complex systems’ resilience. Given this, according to one of the founders of the systems theory, Bogdanov (2003), protecting from external impacts and maintaining internal links are two manifestations of the identic trend. At the same time, Ackoff (1971) emphasizes that the interaction of system elements can lead to different results depending on the specifics and purpose of the relevant elements, as well as the nature of their links. We should also take into account that the orderliness of the whole system depends not only on how well its individual elements function, but also on how its relevant processes are organized. For the purposes of systems analysis, Bertalanffy (1968) singled out system structural order (orderliness of elements) and functional order (orderliness of processes). According to Bogdanov (2003), system changes become more predictable not only because the environment as a source of influence is analyzed but also because the system itself actively influences the environment. Analyzing social systems, the scholar notes that it is necessary to forecast changing external influences and prepare for them not only for success but also for the very existence of such systems. According to O. Bogdanov’s conclusions, organizations should carefully allocate their capabilities to strengthen work in some areas and weaken in others. Here it is expedient to use offensive tactics in an area where environment resistance is expected to weaken and vice versa: where hostile activities are expected to intensify, it is necessary to strengthen protection (Bogdanov, 2003). The aforementioned allows us to conclude that *if the nature and formation features of the links between system elements and its external environment are determined, then public policy in national security and resilience is formed and implemented more effectively*.

1.2.4. Comparative Analysis of the National Security Ensuring System and the National Resilience Ensuring System

After considering the content of the national resilience concept, which links such categories as state, society, national values and interests, threats, and responses, it is expedient to conduct a comparative analysis of the national resilience ensuring system and national security ensuring system. Hence, we should discover interrelationships and differences between these two systems, as well as how to develop specific policy practices that can significantly improve national security (Reznikova, 2018g).

One of the main methods to examine national security issues is a systems approach with the determined necessary conceptual framework and basic system elements: objects, actors, aim, critical parameters, system functions, and management principles. In general, ***national security*** *is protection of national interests and national values from external and internal threats*. There is no established definition of "national security" term worldwide and an exclusive list of areas/components it should cover. The phrase "national security" was introduced into political discourse in 1788 by one of the Founding Fathers of American democracy, A. Hamilton (Hamilton, 1788). Currently, scientists and experts have different approaches to interpreting this term due to its complex, multicomponent, and interdisciplinary nature.

For example, Gorbulin and Kaczynski (2009) define national security as protection of the vital interests of an individual, society, and state in various spheres of activity from internal and external threats, which ensures sustainable and progressive development of the state. Kornievsky (2011) believes that national security is the ability of a state to preserve its integrity, sovereignty, political, economic, social, and other foundations of public life and to act as an independent actor in international relations. Sytnyk (2011) defines national security as protection of the vital interests of human and citizen, society and the state (national interests), which ensures sustainable development of society, timely detection, prevention, and neutralization of threats to national interests in various social and state spheres. Brown (1983) argues that national security is the ability to preserve a nation's physical integrity and territory; maintain its economic relations with the rest of the world on reasonable terms; protect nature, institutions, and governance from adversities; and control its borders.

Holmes (2014) believes that national security is the safekeeping of the nation as a whole. We should add that Western scientific discourse considers a nation primarily as a political rather than an ethnic community (James, 1996).

In general, there are two main research approaches to defining "national security" in the expert community: broad and narrow (traditional). According to the broad approach, national security covers almost all spheres of public life.

The second approach narrows the scope of the concept first of all to the military and foreign components of public policy and focuses mainly on preserving state sovereignty and territorial integrity. The above-mentioned research approaches imply that different key means, methods, mechanisms, and tools of the state should be used to provide national security.

Similarly, approaches to determining key national security objects and actors in the scientific literature may also differ. Most often, national security *objects* include national-level phenomena, processes, and relations that need to be protected and preserved. In a more general manner, the objects of national security can be defined as follows: a human, society, and state. *Actors* that have to take necessary security measures are usually the state represented by its authorized bodies. Citizens, society, enterprises, and organizations may be involved in the implementation of certain tasks in the relevant field in the prescribed manner. All elements of the national security system are interconnected, and the relevant mechanisms begin to function due to the ***national security ensuring system***, which is a set of interacting national security actors, forces, facilities, methods, factors, and purposeful actions that guarantee preservation and strengthening of national values, protection and progressive development of national interests through timely detection, prevention, localization, neutralization, and overcoming of internal and external threats, as well as through providing the effective functioning of the national security system and its components. So, the national security ensuring system is an organizational system that arranges the activities of public authorities, institutions, enterprises, organizations, and other entities that should accomplish national security objectives in the manner prescribed by law (Reznikova, Tsiukalo, Palyvoda, Driomov, and Siomin, 2015).

According to Nyzhnyk, Sytnyk, and Bilous (2000), the national security ensuring system is usually organized by the state on the basis of national legislation. Although various actors interact in such a system, it is the state that plays the key role, sets necessary rules, and regulates the system. Here we can clearly differentiate between the terms of national security objects and actors. If a state becomes an object under threat, then all actors (first of all, the authorized state bodies) must interact with each other and take measures within their purview to protect it. Smolyanyuk (2018) also emphasizes the priority of the state in solving national security and defense problems.

In general, the national security ensuring system is intended to counter threats of various origins and levels. Its actors are the state, represented by the main institutions and authorities (primarily the security and defense sector and the strategic governance sector), as well as civil society, organizations, enterprises, and citizens involved in the relevant tasks. All of them are identical key actors of the national resilience ensuring system. Both systems focus on the existing and potentially likely phenomena, trends, factors, and influences that hinder the preservation of national values and the effective implementation of national interests in all governance spheres, i.e. threats to the national security of any nature and origin.

However, as noted earlier, there is no clear delineation between actors and objects in the national resilience ensuring system. A state, institution, society, individual, organization, or enterprise ceases to be considered exclusively an object under threat when it begins to acquire qualities and capabilities necessary to effectively counter dangerous processes and phenomena and successfully adapts to new security conditions, thereby strengthening its own resilience.

As we know, the national security ensuring system is organized in a clearly *centralized manner*, while the national resilience ensuring system is more *decentralized and flexible*. According to Bogdanov (2003), such methods of organizing complex systems have their advantages and disadvantages.

As the scientist states, centralized systems are able to concentrate efforts (”activities”), and due to linear links between their centers and other elements, their structures are more simple and more stable. But it is harder for the systems to develop, in particular, acquire new characteristics and go beyond the determined model. It is assumed that such systems demonstrate greater efficiency in a predictable environment and planned development. However, too high a concentration in the center weakens its links with the periphery. Besides, links between the other elements are quite weak. According to Bogdanov (2003), this makes the system more vulnerable, especially to environmental influences, and less resilient.

In turn, the adaptability (“plasticity”) of the system gives more flexibility to the links between its elements, which facilitates their regrouping (Bogdanov, 2003). This accelerates system development but, at the same time, leads to its organizational complexity and emergence of vulnerabilities. As Bogdanov (2003) states, increasing “quantitative” resilience causes complexity and heterogeneity of system organization to increase and its “structural” resilience to decrease. It is believed that flexible systems function better in changing environment.

There are differences not only between the nature and principles of interaction between the actors of the national security ensuring system and the national resilience ensuring system. The missions of such systems (the ultimate aims of their activities) also differ. Each of the systems is established to organize activities primarily to provide national security or national resilience, respectively.

The aim of ensuring national security, in general, is the absence of threats and hazards or their surmounting. If a society or a state has suffered significant losses and destruction under adversity, we can consider that the ultimate goal of the national security ensuring system has not been achieved, and the system itself is incapable.

In turn, ***the aim of ensuring national resilience*** is to adapt to threats and rapid changes in the security environment in order to maintain continuous functioning of the main spheres of society and state before, during, and after the crisis.

So, missions of the two systems differ. Providing national resilience implies not the absence but the constant presence of potential or current threats, hazards, and crises. This requires not only the ability to counter them but also to adapt to their permanent or long-term influence.

Measures taken in these systems to achieve a specific aim also have different intentions. An important task of the national security ensuring system is to protect the state, society, and every individual through the authorized state bodies. At the same time, due to the redistribution of responsibilities, providing resilience of people, communities, and organizations is largely their own responsibility. They are the ones that should take basic measures to ensure resilience while the state should facilitate this by providing necessary support.

Emphasizing the differences between these aims, Fjäder (2014) argues that the concepts of national security and national resilience are fundamentally different despite their common features. The scholar concludes that from the public policy-making perspective, the critical question is how to balance the relevant interconnected systems so that they can achieve their goals and make optimal use of resources.

Comparing the core provisions of the human security concept (as currently prevailing in the field of national security) and the national resilience concept, Chandler (2012) points out, in particular, the following fundamental differences: national security focuses mainly on protecting “victims” from threats and crises, responding to the latter, and recovering from them, while national resilience is about eliminating vulnerabilities and possible causes of crises, preventing threats, and preparing for crisis responses. Besides, the main security tools in national security are rights and legal provisions (i.e. direct actions), while in national resilience it is abilities and capabilities (i.e. indirect actions). In the national security system, organizational links are built according to the “top-down” principle (the state concentrates key powers), while in the national resilience system – according to the “bottom-up” principle (the powers are distributed) (Chandler, 2012).

In general, *national security ensuring system and national resilience ensuring system are compatible: they can interact and complement each other*. Here, a *synergetic effect* appears: the national security ensuring system acquires new properties enabling it to significantly improve countering modern threats and hazards.

This conclusion is based, in particular, on the research of Lewes (1875) on the emergence and development of this concept in the complex systems theory, as well as on the works of Bertalanffy (1968), Bogdanov (2003), Corning (2002), and others that claim that interaction of several elements within the system result in exceeding the sum of individual actions, and the system itself acquires new properties that were not inherent in individual elements. Thus, there is an effect of increasing interaction between different factors with coinciding vectors. According to Corning (2002), the main ways to achieve synergistic effects are as follows: functional complementarity of similar activities; a combination of different types of activities; and scale effect (a set of elements produces a unique joint result).

Analyzing the current practices in providing national security, we can conclude that some non-systematized measures are taken within this sphere, which can be generally attributed to ensuring national resilience. In particular, we can speak about periodic reviewing and updating national security strategies and the relevant program documents, forming necessary reserves and emergency plans, and plans for special periods. Nyzhnyk, Sytnyk, and Bilous (2000) argue that the critical parameters of the national security system should also cover resilience of the basic social system characteristics: protecting the constitutional order, adjusting the determined procedures for normalizing ongoing changes, providing the succession of power, and social policy in general.

Regarding the protection of the basic social system characteristics – sovereignty, territorial integrity, and inviolability of the state border – it would be more appropriate to speak about their steadfastness and resistance rather than resilience. The relevant objects need, first of all, protection provided by foreign policy and hard power. Here, national resilience ensuring measures can be used mainly in the form of strengthening, if necessary, national security and defense sector capabilities, using alternative security strategies, asymmetric indirect impacts, and strengthening external ties.

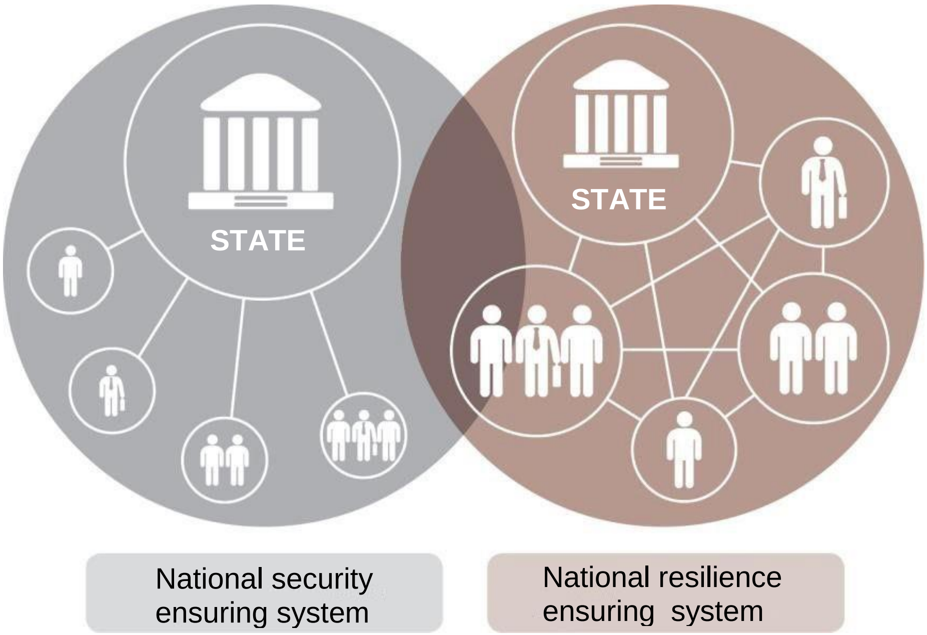
According to Fjäder (2014), security and reliability are important elements of national resilience, reducing the likelihood (prevent) of an emerging crisis, limiting its impact to avoid irreparable damage and fatalities, and facilitating rapid recovery by securing critical structures and resources. At the same time, resilience can be considered an integrated element of national security allowing to provide preparedness for unpredictable and sudden threats when it is impossible or at least uneconomic to use a preventive approach to security. Fjäder (2014) summarizes that in contrast to national security, national resilience is about creating conditions that will guarantee at least minimal stability in meeting basic social needs until adverse impacts of crises and hazards are eliminated. Thus, the scholar proposes to consider national resilience as a resource-efficient national security guarantee in the face of the recognized risk of uncertainty.

So, the analysis conducted within this study allows us to argue that national security and national resilience ensuring systems have both common and distinctive features (Reznikova, 2018d, 2018g). In general, these systems consist of the same actors and have a certain similarity of objects, but differ in mission, organization of links between actors, and mechanisms.

Within traditional national security ensuring system, the state performs basic functions, and other actors (citizens, civil society, organizations, enterprises, etc.) are involved in certain tasks if necessary (i.e., in case of mobilization or to perform democratic civilian control). That is, the relevant links are formed according to the “top-down” principle. The national resilience ensuring system redistributes certain powers, and actors exercise more powers on a permanent basis. Links between the actors become more complex and become especially significant in the national resilience ensuring system. Here, an important task for the state is to establish coordination, concerted functioning, and effective interaction between the existing or emerging national systems, state and local authorities, and other entities to address common challenges in providing national security and resilience. That is, the relevant links are formed according to the “bottom-up” principle.

In general, traditional exclusive approaches are more suitable for solving a range of tasks in national security, especially those in which the state plays a leading role. At the same time, other mechanisms based on resilience and inclusiveness should be offered to respond to new threats (especially hybrid ones) as well. This approach is especially relevant for solving tasks that require interaction of various actors (first of all, state and local authorities, civil society organizations, business representatives, and individuals) or allocation of responsibilities. Fig. 1.2 schematically shows the formation features of the national security ensuring system and the national resilience ensuring system (including the weight of key system elements and the nature of systemic links) and their possible interaction.

Fig. 1.2. Possible interactions of the national resilience ensuring system with the national security ensuring system with due account for their features


STATE
STATE
National security ensuring system
National resilience ensuring system

Source: developed by the author.

Given the compatibility of national security ensuring system and national resilience ensuring system, it can be argued that by forming and implementing state policy in national resilience and implementing the relevant mechanisms we can strengthen the national security system by giving it a new quality that better meets the current conditions of uncertainty and high-turbulent environment.

1.3. Theoretical Basis for Assessing and Managing National Resilience

1.3.1. National Resilience Criteria

The national resilience ensuring system can be identified, in particular, by such system parameters as national resilience *criteria* and the *principles*. The resilience of the system objects is formed as they acquire a set of necessary qualities – fundamentally important characteristics that allow us to identify resilience and distinguish it from other statuses or processes inherent in the state and society. Ways to achieve these parameters determine the nature of national resilience ensuring *mechanisms*, which allow the relevant system to fulfill its mission.

There are different approaches to defining the **national resilience criteria** in the expert community due to different interpretations of the national resilience concept. Let's consider the key criteria of national resilience.

Adaptability (i.e. the ability to withstand impacts and adapt to a change in environment through certain internal changes) is one of the most important characteristics of a complex system's resilience, which allows the system to preserve its integrity and continue to function.

In addition to this criterion, Uyemov (1969) also includes the system's simplicity or complexity, its reliability, stability of the structure, individual elements, and system links in the parameters associated with the system's resilience. Fiksel (2003) determines the following system resilience criteria: diversity (existence of multiple forms and behaviors of the system), efficiency (performance with modest resource consumption), adaptability (flexibility to change in response to new pressures), and cohesion (existence of unifying forces or linkages).

A special report on building national resilience to global risks, compiled by a team of scholars as part of the World Economic Forum's annual report (WEF, 2013), identified five key national resilience criteria, grouped in two clusters:

1) resilience characteristics:

- robustness;
- redundancy;
- resourcefulness;

2) resilience performance:

- response;
- recovery.

The Resilience Alliance (2010) defines the following important criteria for assessing the social-ecological systems resilience: diversity, openness, tightness of feedbacks, system reserves, and modularity.

Thus, the above-mentioned research approaches to determining complex systems' resilience criteria reflect the main characteristics inherent in a resilient system.

In further research on the determining resilience criteria, Rensel (2015) offers a detailed classification of these criteria depending on the characteristics of their application: the criteria of purpose, status, processes, and system interaction. The scholar developed a resilience matrix, which is an operational tool and can set system parameters which, if achieved, ensure the system's resilience at a level determined by key criteria of its operation: system parameters (overview, normal operation, protection, corrective actions, vulnerabilities, planning, mitigations, and vigilance), confidence, security, continuity of operations, and preparedness. So, according to Rensel (2015), the system resilience is assessed in terms of the system's key functions and processes from the perspective of their sufficiency or insufficiency to achieve the assigned goal or ensure business continuity.

Accordingly, the achievement of resilience criteria by an object can be assessed differently depending on the state of the system. In particular, the scholar identifies the following resilience *states*: exposed; confusion; aware; operational; capable.

Other researchers (Proag, 2014; Rose, 2007) offer alternative approaches to determining the resilience criteria of complex systems. They are usually relevant to a particular field of activity and can be used to characterize the state of certain components of the country and society or processes that take place within the national resilience ensuring system.

Recognizing that specific criteria may be used to characterize the resilience of individual subsystems and elements of the state and society as complex systems, based on the generalization of current theoretical research and world practices, it is expedient to determine the *basic criteria of national resilience*. They can be used to characterize various fields, subsystems, organizations, complexes, and processes in national security as well as in the national resilience ensuring system in general. It is expedient to include the following criteria in the list of the basic criteria of national resilience:

resilience criteria of the object's state:

- robustness;
- redundancy;
- adaptability;
- absorption;

resilience criteria of the object's functioning

- preparedness;
- rapidity;
- response;
- recovery.

In general, the above criteria characterize the following key *features of national resilience:*

- the ability of the state and society to effectively respond to threats and crises, ensure sustainable (continuous) functioning and development of key areas, anticipate risks, and overcome obstacles arising from adverse impacts/threats (reliability);
- the availability of additional capabilities that may be involved in case primary and alternative plans fail, as well as development strategies for crises, and safety margin (redundancy);

- the ability of the state and society to ensure survival in crises and adapt to adversities without significant loss of functionality; the ability to transform negative results into positive ones, apply non-traditional, innovative, and inclusive solutions (adaptability);
- the ability of the state and society to neutralize destructive influences and prevent threats (absorption);
- the ability of state servants and citizens to study, learn lessons from the exercises, training, and experience of overcoming threats and crises, establish effective communication and broad liaisons, and plan joint measures to respond to threats and crises (readiness);
- the ability of state servants and citizens to join efforts and effectively respond in a threat or crisis; cohesion; adherence to protocols of concerted action (response);
- the ability of the state and society to restore sustainable functioning of the main spheres of life after crises at a level not lower than pre-crisis; adaptation to new circumstances arising under the destructive influence of a crisis; development (recovery);
- providing rapid access to resources, their mobilization in crisis, and high rates of post-crisis recovery (rapidity).

Summarizing the above, we can conclude that in general, a state can be considered resilient if it is able to:

- function continuously in the normal mode; adapt to changing conditions;
- withstand unexpected blows;
- recover quickly from destructive impacts of threats and crises of any nature and origin to a determined equilibrium (at the previous or new level) while maintaining management continuity;
- develop under difficult security circumstances (Reznikova, 2017).

The above-mentioned basic criteria of national resilience can be used to assess the resilience of various branches, institutions, organizations, and complexes in relation to various threats and crises. At the same time, to assess *society's resilience* we should add a few more features important for determining the nature of social relations.

Having analyzed scientific sources, we may argue that there are some differences in ensuring the resilience of the state and the resilience of society. According to a number of researchers, including Polasky, Carpenter, Folke and Keeler (2011), a set of resilient individuals does not guarantee social resilience. At first glance, this statement contradicts the classical systems theory, which holds that a system's functioning result is greater than a simple sum of its individual elements' results. But at the same time, this judgment emphasizes the special importance of system links and behavior management in society.

According to Brown and Kulig (1996/97), people are resilient when they are together.

The authors of the "Report of criteria for evaluating resilience" (Pursiainen & Rød (Eds.), 2016) note that today there are no generally accepted criteria to assess the resilience of society and communities. Those proposed by various researchers are mostly just a list of general socio-economic and institutional-political indicators related to crisis management or the ability of communities to defend themselves.

The aggregated potential of a society or community (social capital) is often considered a basis to assess social resilience. It covers primarily economic, social, and environmental capital, in the context of which specific criteria and indicators are determined. Wilson (2012) argues that economic capital is characterized by economic prosperity, business diversification, budget dependence on external financing, etc.; social capital is characterized by the strength of social ties, access to educational and medical services, corruption level, communication between the main actors, etc.; environmental capital is characterized through biodiversity, quality, and availability of water resources, predictability of yields, etc.

In addition to the economic and social capital of a society, scholars, including Norris et al. (2008), identify the following important components of social resilience: information and communication (narratives, responsible media, information infrastructure, traditions and skills of the population to use basic information sources, and credible information resources); social responsibility (social proactivity, ability to solve problems together, flexibility and creativity, joint strength and authority, and partnership) and more. According to Norris et al. (2008), the economic capital of a society or community includes, in particular, the level and diversity of resources, as well as their fair distribution; social capital includes the possibility of receiving real and potential social support, social involvement (informal ties), organized (formal) ties and cooperation, community participation, leadership and responsibility, community sense, and attachment to a particular territory. Considering social resilience as a process that ensures the security and well-being of citizens, increases their readiness and effectiveness in responding to threats and emergencies, these scholars suggest taking into account such criteria as reliability, redundancy, and rapidity (including rapidity of access to resources and their mobility) when analyzing the above-mentions social resilience components.

There is a close link between social resilience and community resilience, on the one hand, and the resilience of organizations that ensure their safety and provide critical services, on the other. In particular, Lee, Vargo and Seville (2013) pay attention to this. According to the researchers’ conclusion, in order to be resilient, organizations have to meet certain criteria, i.e. have strong leadership, be aware of the environment in which they function, have the ability to overcome vulnerabilities and adapt to rapid change. The ability of organizations to overcome social, cultural, and behavioral barriers that hinder effective communication is also important in today’s world.

Summarizing the above, it is expedient to determine *key criteria of social resilience* as follows:

resilience criteria of the state of society/community:

- identity;
- coherence and unity;
- ties between different social groups;
- involvement of the population in economic, political, and other activities within the state and community;
- confidence in authorities;

resilience criteria of functioning of society/community

- effective community management;
- citizens' awareness of the nature of threats, as well as the procedure in case of their occurrence;
- readiness to respond;
- controllability of the situation before, during, and after a crisis;
- creating joint capabilities to counter a threat or crisis.

Table 1.3 shows a classification of basic criteria of national resilience depending on the type of objects in terms of the main components of the state and society, as well as their state or functionability, which are the defining characteristics of resilience in national security. The proposed methodology for determining the basic criteria of national resilience has interdisciplinary nature and can be used as a basis to develop criteria of specified resilience related to various areas, objects, and spheres of public relations.

Table 1.3

Classification of Basic Criteria of National Resilience

Objects	Resilience criteria of the object's state	Resilience criteria of the object's functioning
Branches, subsystems, technical complexes, organizations, processes, the	• reliability; • redundancy; • adaptability;	• preparedness; • rapidity; • response;

national resilience ensuring system, etc.	• absorption	• recovery
Society, communities, social groups, etc.	• identity; • coherence and unity; • ties between different social groups; • involvement of the population in economic, political, and other activities within the state and community; • confidence in authorities	• effective community management; • citizens' awareness of the nature of threats, as well as the procedure in case of their occurrence; • readiness to respond; • controllability of the situation before, during, and after a crisis; • creating joint capabilities to counter a threat or crisis

Source: developed by the author.

To study the resilience of different target groups (communities, organizations, populations, etc.) and branches to certain threats or destructive impacts deeper, detailed criteria can be developed that characterize the specifics of the selected group or branch and its response to relevant threats and impacts (for example, resilience criteria of rural and urban populations to disinformation, critical infrastructure resilience to the terrorist threats, etc.)

1.3.2. Resilience Indicators and Levels in National Security

Based on the basic criteria, we may develop appropriate resilience *indicators* and determine resilience *levels*. It should be noted that researchers define the following main conceptual approaches to determining indicators and levels of resilience: recognition of resilience as a certain system *state* or as a *process* aimed to achieve the formulated goal. Besides, there are other peculiarities and differences in determining resilience indicators and levels of complex systems.

In general, both specified resilience and general resilience of a system can be assessed. According to the Resilience Alliance (2010), *specified resilience* is the resilience of different objects to different threats or impacts, while *general resilience* characterizes the system as a whole.

It would be reasonable to distinguish two subtypes of specified resilience on the following grounds:

- object's resilience to certain types of threats and crises (for example, resilience of a state and its subsystems to terrorism, droughts, floods, economic crises, and information attacks);
- resilience of a certain object to a wide range of threats and crises (for example, organizational resilience, community resilience, and social resilience)

The Resilience Alliance (2010) has developed a comprehensive methodology to assess the resilience of social-ecological systems based on identification of key system elements and links between them, including aims and motivations of various actors and factors influencing the system state.

According to this research approach, the lists of questions have been formulated allowing to:

- assess the state of various subsystems and elements, characterize adversities, and determine if certain problems exist;
- identify factors influencing the whole system and the scope of possible changes (including temporal and spatial);
- identify and evaluate cascading effects within a complex system; evaluate the condition and effectiveness of system management, and in particular, identify formal and informal links between key actors.

The Resilience Alliance (2010) emphasizes that the proposed questionnaires are tailored. They need to be adjusted with due account for the characteristics of the examined object (specific subsystem). According to the Resilience Alliance (2010), appropriate resilience-strengthening strategies should be developed based on the analysis of assessment findings.

Having analyzed the above researches, we can conclude that *assessing national resilience is a complex and comprehensive process that combines* *assessing conditions of various subsystems and processes within the state and society, identifying and assessing risks and vulnerabilities, determining the optimal and acceptable balance of the state and society and their relevant resilience levels*. As methodologies for assessing different subsystems and areas of public relations may significantly vary, the question arises if it is possible to harmonize them and compare their results. These problems will be addressed in Chapter 2 of this monograph.

It is expedient to use **indicators** within the above-mentioned basic criteria to assess national resilience. Generally, indicators should reflect peculiarities of the branch, object, or process they will be applied to. That is, we are talking about specified resilience indicators. Therefore, it is expedient to use the method of decomposition of the national resilience system and its objects in order to develop such indicators.

In particular, the Resilience Alliance (2010) suggests considering, among others, the following important indicators that can be used to characterize social-ecological systems' resilience:

- the number of adverse effects that the system can absorb without significantly upsetting its balance;
- the level of the system's ability to self-organize;
- the level of the system's ability to learn and adapt.

Carpenter, Walker, Anderies, and Abel (2001) emphasized the important difference between resilience indicators and other ones. According to them, resilience indicators should focus on variables that describe the system's potential to provide system services (in the case of social-ecological systems – the ecosystem services), while other indicators mainly relate only to the current condition of the system or service.

Today, various international organizations, research centers, and individual scientists develop and offer numerous resilience indicators, which can be used in the national security field. These are, in particular, resilience indicators of branches and institutions (Jovanovich et al., 2016; Prior & Hagmann, 2012), business processes (IBM, 2009), and operational services (Rensel, 2015). On their basis, certain indices of the resilience of states (FM Global, n.d.), cities (City resilience index, n.d.), and security and resilience standards (ISO, 2007a, 2007b, 2013, 2019a) are formulated. However, there are currently no universal indicators of national resilience.

Other important system parameters on which national resilience ensuring mechanisms should be focused are **resilience levels**. The level estimates can be benchmarks in formulating public policy in the field of national security and resilience. For example, comparing the current object resilience level with an acceptable risk level will help detect vulnerabilities in the state and society. These estimates also allow determining the need to apply certain mechanisms and practices and the amount of resources required for their implementation.

A common method of assessing the resilience level of a complex system is to develop indicators based on the results of generalized expert evaluation according to the selected criteria. This is due to the fact that a large number of risks and threats (especially hybrid), as well as the system characteristics that allow systems to resist or adapt to adverse effects, cannot be statistically estimated. Results of such evaluation are usually somewhat subjective. Given this, the relevant evaluations cannot be perceived as completely reliable but should be considered as the most probable vector of system development. They demonstrate the system's strengths and weaknesses allowing to choose the best strategy for providing the system's resilience.

Considering the above-mentioned research approach, the level of national resilience or the corresponding index (general system resilience index) should be aggregated indicators consisting of estimates of resilience levels in different branches and sectors (specified resilience indices). Criteria for assessing national resilience level should reflect, on the one hand, the specifics of the selected branch/sector, and, on the other, take into account the basic resilience criteria of the system's state and system's functioning, which were mentioned above.

Another research approach to determining resilience level is to form a list of fundamentally important characteristics of processes and states (benchmarks) that should be achieved to obtain the optimal level of resilience under the determined conditions. According to this approach, the system and its components are assessed during periodic benchmarking.

Based on the above, we can conclude that the need to achieve the established criteria, identify priority areas and optimal level of national resilience, as well as the acceptable risk level and possible losses, is the basis to form mechanisms allowing national resilience parameters to achieve the determined benchmarks. Here we should take into account that the *optimal resilience level varies depending on the objects. The level of an object's resilience to different types of threats, in particular, in different times and contexts, may also vary*.

Holling (2001), Hayek (1967, 1991), Walker and Cooper (2011), Carpenter and Brock (2008), Bowles, Durlauf and Hoff (2006), Erikson (1995) and other researchers draw attention to certain *resilience traps*. First of all, there are extreme cases when a certain system (for example, a state) can be too weak (poverty trap) or too rigid (rigidity trap). Both cases make it impossible to further change the system, its adaptation and development in order to effectively respond to destructive influences and threats. To support their conclusions, these scholars cited the example of a fully decentralized liberal system of government and a totalitarian regime.

Carpenter and Brock (2008) discovered that rigidity traps have the following features: low diversity of system elements, rigid links between them (hierarchy), high ability to focus on a single problem-solving approach, and low ability to develop alternative solutions. All this reduces the system's ability to adapt and increases the risk of its destruction. Such conditions are characterized by high resistance. For example, biological organisms may stop responding to medicines that have been used for a long time against a particular disease making them more vulnerable to it and limiting treatment mechanisms. In extreme cases, this leads to death.

Carpenter and Brock (2008) also noted that insufficient resilience (poverty) traps are characterized by a significant diversity of system elements with weak links between them. This reduces the ability to mobilize problem- solving ideas and resources. And too weak control combined with significant variability of possible solutions does not allow focusing on the optimal solution to the current problem. For example, this may lead to neglecting public interests in favor of individual or corporate ones. According to Carpenter and Brock (2008), insufficient resilience (poverty) traps indicate the unrealized potential of the system.

Based on the above theoretical conclusions, we can assume that a complex social system cannot have zero resilience level even if it falls into a resilience trap. If we assume such a situation, it would mean the absence of system links between the complex system’s elements and, therefore, its inability to function and maintain integrity. Obviously, all existing systems have a certain level of resilience, which can be higher or lower depending on various circumstances and influencing factors. So, within the interdisciplinary resilience concept, it is incorrect to say that a complex system, such as a state, is not resilient. Even in the case of a failed state, it is advisable to equate it with one that has fallen into the resilience trap until it ceases to exist or transforms totally.

In the context of the system resilience level discourse, Bourbeau (2013) concludes that protection from dangers and shocks cannot be guaranteed completely, and no society can be completely resilient. Chandler (2012) agrees, saying that it is impossible to achieve complete resilience: this is just a continuous process with an assigned aim.

To determine the national resilience level, it is important to pay attention to the conclusions of Bogdanov (2003) on the peculiarities of complex systems functioning. According to the law, he elaborated, the structural resilience of a whole system is determined by the lowest resilience of its comprising elements (the law of the least relative resistances, or the law of minimum). This is about a limiting factor that determines, in particular, the rate of system recovery after disrupting effects. Extrapolating Bogdanov's conclusions to the national resilience system, we can argue that if one of the system's elements remains non-resilient, it may point to vulnerabilities, in particular in the state, its subsystems, and society. In view of this, and given that key national resilience system objects are complex systems, it is important to assess the resilience of each of their elements (including individual branches, subsystems, critical processes, public authorities, and communities).

The results of the above research show that the ability of the system to adapt, as well as its resilience level, can change. This raises a concern about how to influence the processes of providing objects' resilience without falling into resilience traps and guiding the system development in a determined direction.

1.3.3. Fundamentals of National Resilience Management

In general, the resilience level of a complex system depends on its organizational features, the type of threats and adversities it faces, as well as the targeted actions of resilience ensuring actors (key actors). In the context of providing national resilience, the activities of such actors are determined by aims and objectives that form the basis of state policy in this area. The effectiveness of such a policy largely depends on whether it corresponds to the content of the national resilience concept and whether it takes into account national resilience management regularities.

In this context, Bogdanov's "law of minimum" deserves attention.

According to it, the most destructive effects concentrate on the weakest links. This causes the greatest system resistance (Bogdanov, 2003). In the context of national security policy formation, this law encourages looking for solutions aimed not only at timely detecting vulnerabilities but also at optimizing capabilities directed at recovering from destructive impacts.

Bogdanov (2003) also identified the main ways to overcome the relevant system weaknesses: 1) under anticipated influences (forces) with a determined trajectory, it is logical to systematically strengthen the "weak links;" 2) in conditions of uncertainty, the uneven concentration of capabilities in favor of some and to the detriment of others is pointless and dangerous, as it increases the probability of destructive results even from quite weak impacts on the most unreliable system elements. Relative resilience is maximized through even distribution of capabilities between all endangered links of the whole system.

The Resilience Alliance (2010) expresses a similar caution, arguing that if all attention and management resources are focused on managing resilience to certain types of influences and consequent obstacles, management actions may inadvertently reduce the resilience of the system as a whole. For example, if you strive to be highly resilient to the destructive influence of a certain type, then the system's ability to cope with unexpected or completely new threats may decrease.

Complex systems are able to *self-organize* and *self-manage*, which allows them to counter influences and return to equilibrium. This is a basis for the *"embedded" resilience* of complex systems. This system potential can be increased, in particular, through purposeful actions of the national resilience actors or synergistic effect from liaisons with other systems. This added value is the *"acquired" resilience (Fig. 1.3)*.

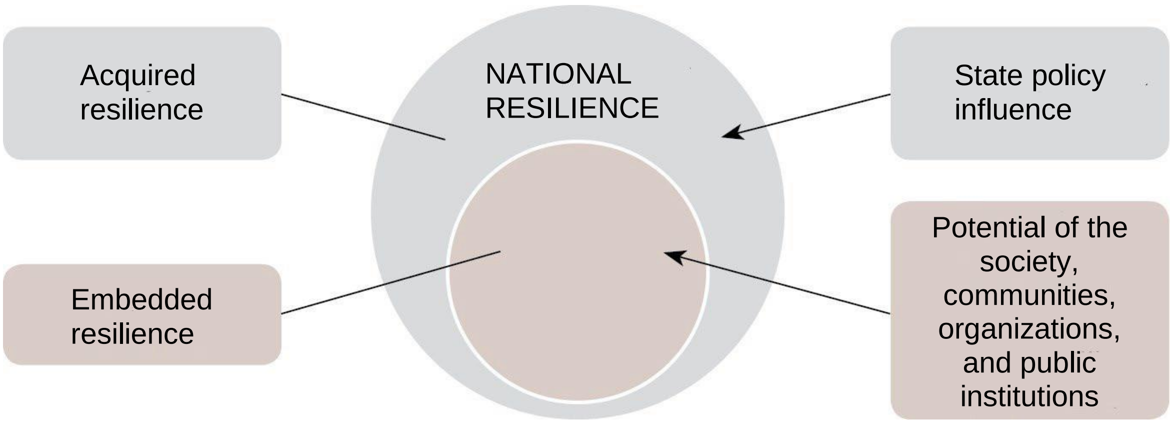


Fig. 1.3. Resilience types by their origin

Source: developed by the author.

Purposeful actions of national resilience actors can change the resilience level of different objects in a certain way. The relevant processes are determined by the laws of systems *adaptive behavior* and *adaptive management* formulated within the complex systems theory.

Ashby (1960) explains the adaptability phenomenon by the peculiarities of the adaptive behavior of biological organisms as complex systems: each mechanism adapts to function according to its purpose; and in general, the mechanism aims to maintain important system parameters (variables) within the determined limits. According to the scientist’s conclusions, adaptive behavior equals the behavior of a stable system that functions in an environment where all significant variables are within their normal values (homeostatic range).

Extrapolating these findings to complex social systems, we can argue that they are able to self-organize and, to some extent, to self-govern. This corresponds to Bertalanffy’s conclusions (Bertalanffy, 1968) about such important complex systems characteristics as equifinality (a trend to achieve an end state which allows acquiring stability starting from different initial conditions and using different ways based on dynamic interaction in an open system) and feedback (homeostatic support of the system’s stability on the basis of circular causal connections and mechanisms for monitoring feedback on deviations from the condition which should be maintained). According to Bertalanffy (1968), a situation when a system restarts on the basis of a new behavior or operating rules after having overpassed critical values can be an example of adaptive behavior.

However, we should not assume that self-organization and self- governance is the best option for the state and society as complex systems to exist and develop. Governance and social development remain extremely important, especially in national security. Under a wide range of threats and changing security environment, it is expedient to use adaptive management, which, according to Holling (1978), combines the understanding of problems, concepts for solving them, and processes and methods for adaptive assessment and management. It is a flexible adaptive policy-making process, partly aimed at reducing uncertainty. Here, the scientist points out that *assessment as an integral part of adaptive management is particularly important*. Assessment should be carried out continuously during the implementation of the relevant policy or project and provide information essential for selecting and adjusting ways of further development. This is how policy should be adjusted (Holling, 1978).

According to Habron (2003), the Resilience Alliance (n.d.a), and Walters (1986), adaptive management identifies uncertainties and then establishes methodologies to test hypotheses concerning those uncertainties. This process implies the openness and involvement of a wide range of stakeholders. It aims to increase institutional flexibility and encourage forming new institutions required to use this understanding on a daily basis. To this end, adaptive governance must be both a social and scientific process focused on the development of new institutions and institutional strategies, scientific hypotheses, and experimental frameworks. Adaptive management can enhance the overall system resilience by increasing its flexibility, inclusiveness, diversity, and innovation (Habron, 2003; Resilience Alliance, n.d.a; Walters, 1986).

Bourbeau (2013) identifies three *resilience types* according to actor- defined aims and the amount of effort required to achieve them:

1) resilience as maintenance, which implies such a level of object adaptation at which the available resources and actions will be directed towards maintaining the status quo in the new circumstances (for example, strengthening certain measures within the state policy under implementation);
2) resilience as marginality, which implies responses that bring changes at the margins of an object's functioning (in particular, within the current state policy, regulations, and social structure) that will not affect its systemic parameters (e.g., organizational, institutional, political, and other foundations of society);
3) resilience as renewal, which implies a transformation of basic foundations of the object (e.g., public policy priorities or social structure of society) according to new conditions of development and transition to a new equilibrium.

According to the Resilience Alliance (2010), systems can move from one equilibrium to another, going beyond certain limits. Such movement can be abrupt and unexpected or carefully planned. With this in mind, it is important to know how to push change in order to achieve the determined aim and desired equilibrium. In the context of providing national resilience, it is a matter of determining the relevant public policy priorities.

According to the classification proposed by Bourbeau (2013), we can, in particular, determine various national resilience dimensions in national security policy-making. Given that the first two types of resilience have a more fragmented nature (a specific threat affecting a specific object), it is more expedient to talk about strengthening specified resilience (resilience of the state, society, organization, critical infrastructure, etc.). This means that a set of resilient objects and actors should be formed to ensure national resilience, which implies that measures aimed to strengthen certain spheres and areas of national security (the first resilience type), as well as to reform the national security and defense sector (the second resilience type) should be developed and implemented. More effort is required to apply an integrated approach to providing national resilience, especially in countries that face a wide range of threats. It is usually associated with some changes in the social relationships system, including security. This approach is more in line with achieving the third resilience level proposed by Bourbeau (2013).

So, based on the above, we can argue that in the context of adaptive management in national resilience, providing the first level of resilience implies constant monitoring of national security threats, timely detection of dangerous trends, situation analysis, and preparation (adjustment) of action plans (including alternative ones) if the threat level increases.

The second level of national resilience must be ensured when a threat is permanent, but its consequences will moderately impact the society, or if its level tends to exceed the established limits. This requires strengthening national security and defense sector capabilities, providing continuous public awareness about the nature and dynamics of threats and about operating procedures in case they materialize, creating sufficient emergency reserves, and conducting appropriate training, exercises, and other activities within the limits defined by law.

In order to achieve the third level of national resilience, a large-scale reform of the national security ensuring system or its components and mechanisms is required. This, in turn, should aim to provide continuity in governance, continuous functioning of all life-support systems, and social relations during crises, as well as their rapid recovery after a crisis, at least to the previous level.

Bourbeau (2013) points out that these resilience types can exist in a state or society simultaneously or by turns. Summarizing the above, we can assert that it is expedient to combine the above-mentioned different groups of measures to achieve the determined aim and create a basis for a comprehensive national security and resilience policy.

1.3.4. Factors Influencing the Formation of National Resilience

In addition to the targeted actions of resilience actors, a number of other **factors**, including time, situation context, and system constraints (in particular geographical scope) may influence the level of resilience, which can be considered sufficient for a system to sustainably function and develop.

According to the Resilience Alliance (2010), it is more important to know what factors push a system out of the existing equilibrium limits than those that break such limits.

The discovery of the *adaptive cycle* of complex systems development allowed finding out regularities that determine the different effectiveness of influence on the complex systems' resilience in different cycle phases. The adaptive cycle alternates between slow and gradual phases of growth and accumulation and shorter innovation-enabling periods of reorganization.

Interventions at different stages of the adaptive cycle may have different consequences for system development. In view of this, according to Gunderson, Holling, and Light (1995), there is a "window of opportunity" to respond – a period with the highest effectiveness of system resilience strengthening actions within an adaptive cycle.

Bourbeau (2013) draws attention to another national resilience feature: resilience depends on the *time and context of the situation*. Thus, the same event (phenomenon, trend) may pose a threat (for example, migration as an excessive burden on national social and healthcare systems) to one state while not posing a threat to another (for example, migration as an influx of skilled workers into the domestic market). The event may also be treated differently in different periods (for example, migration in conditions of sustainable development or armed conflict). Bourbeau (2013) gives another example: a soldier can be considered a resilient actor in an armed conflict or emergency (because of the appropriate training) but have much less resilience, including psychological, as a civilian (while on leave or after demobilization).

Formulating the law of least relative resistance (law of minimum), Bogdanov (2003) argued that the interaction of the system with the environment should be considered as changing over time, therefore, the resilience of the system as a whole depends on the resilience of its weakest link in a specific period.

Based on the above, we can conclude that the *time factor and the context of a situation are variables that should be considered in adaptive management in national security and resilience and formulating the relevant state policy*. In particular, it is important to establish and periodically review which level of national resilience can be considered sufficient under the determined conditions, including that of certain subsystems and elements of the state and society.

The influence of the time factor on the processes of determining the system's ways of development *forms permanent links between past, present, and future*. According to the observations of a range of researchers, including Bourbeau (2013), Gunderson and Holling (2001), Gunderson, Holling, and Light (1995), Kaufmann, Cavelti, and Kristensen (2015), past events often determine current actions and affect future plans.

In particular, Bourbeau (2013) argues that a system changes its equilibrium with a corresponding readjustment of system parameters based on the experience of past events, collective memory, and social history, which is crucial for decision-making in new circumstances.

Learning lessons from the past, including disasters and crises, is important to create and develop the capabilities necessary to counter current and future threats and function effectively under chronic stress and uncertainty. For example, mandatory investigations of aviation accidents according to International Civil Aviation Organization (ICAO) requirements aim to improve aviation safety by eliminating possible shortcomings in the organization of transportation, aircraft design, and staff training. Based on the lessons learned, the recommendations allow strengthening the resilience of both aircraft and aviation transportation systems in general against likely threats of various nature and origin (design flaws, terrorist attacks, and dangerous natural phenomena).

However, it is important not to fall into certain institutional and other traps, mentioned, in particular, by Ashby (1947). He argued that it made sense to reproduce a previously gained experience only if the events were similar. If a system faces completely new challenges and threats, then actions under the old pattern are inappropriate or even harmful to provide system resilience or development.

This conclusion is crucial to forming the national resilience ensuring system in modern conditions characterized by high variability and uncertainty of the security environment. This means that national security policy must be flexible enough.

Attention should also be drawn to other traps in providing national resilience. In particular, Martin-Breen and Anderies (2011) note that this process may be accompanied by a conflict of aims and values, including in the temporal dimension. The point is that by focusing only on solving current problems in the state and society in order to strengthen national resilience, we can significantly deplete resources or create new problems in the long run. For example, using certain medicines to prevent dangerous diseases from spreading can weaken people’s immunity and make their bodies insensitive to the necessary treatment in the future, while strict long-time quarantine restrictions can cause significant economic damage. Besides, given the wide range of current threats and crises and limited financial resources, we have to choose both between the aims and objectives of state policy in various fields and between aims in providing national resilience (e.g. strengthening critical infrastructure or social resilience). This foregrounds an issue of prioritizing the relevant aims and objectives of state policy in various sectors under the existing resource constraints.

Factors influencing national resilience can also be formed during the interaction of the national resilience ensuring system with other systems. In particular, governance, political, and economic processes may influence the level of national resilience. WEF (2013) identified key factors of these influences:

- politicians' ability to govern;
- business-government relations;
- reform implementation efficiency;
- public trust of politicians;
- wastefulness of government spending;
- measures to combat corruption and bribery;
- government provision of services for improved business performance.

Among other factors that influence the formation of national resilience we should mention those that characterize social development processes, namely:

- peculiarities of national mentality;
- general level of education of the population;
- standard of living;
- prevalence and availability of media and other sources of information;
- sophistication of social ties;
- society self-organization level, etc.

All these factors may both strengthen national resilience providing processes and diminish their end results.

Based on the above, we can conclude that it is expedient to apply an integrated approach to managing the national resilience level. We primarily argue that it is necessary to periodically assess the resilience of key objects and their components for their compliance with the determined indicators in terms of basic national resilience criteria. Even if the objects meet these criteria, the optimal and permissible national resilience levels should be adjusted with due account for the findings of the analysis of various factors of influence (time, situation context, etc.). In order to determine measures required to adjust the national resilience level and/or bring the resilience of major objects and their components in line with the basic national resilience criteria, it is necessary to identify an adaptive cycle phase of the state and society. This will allow applying the most effective measures in a determined period. Besides, it is expedient to eliminate or minimize the adverse influences on national resilience from other systems if possible. *Fig. 1.4* shows the general national resilience management algorithm.

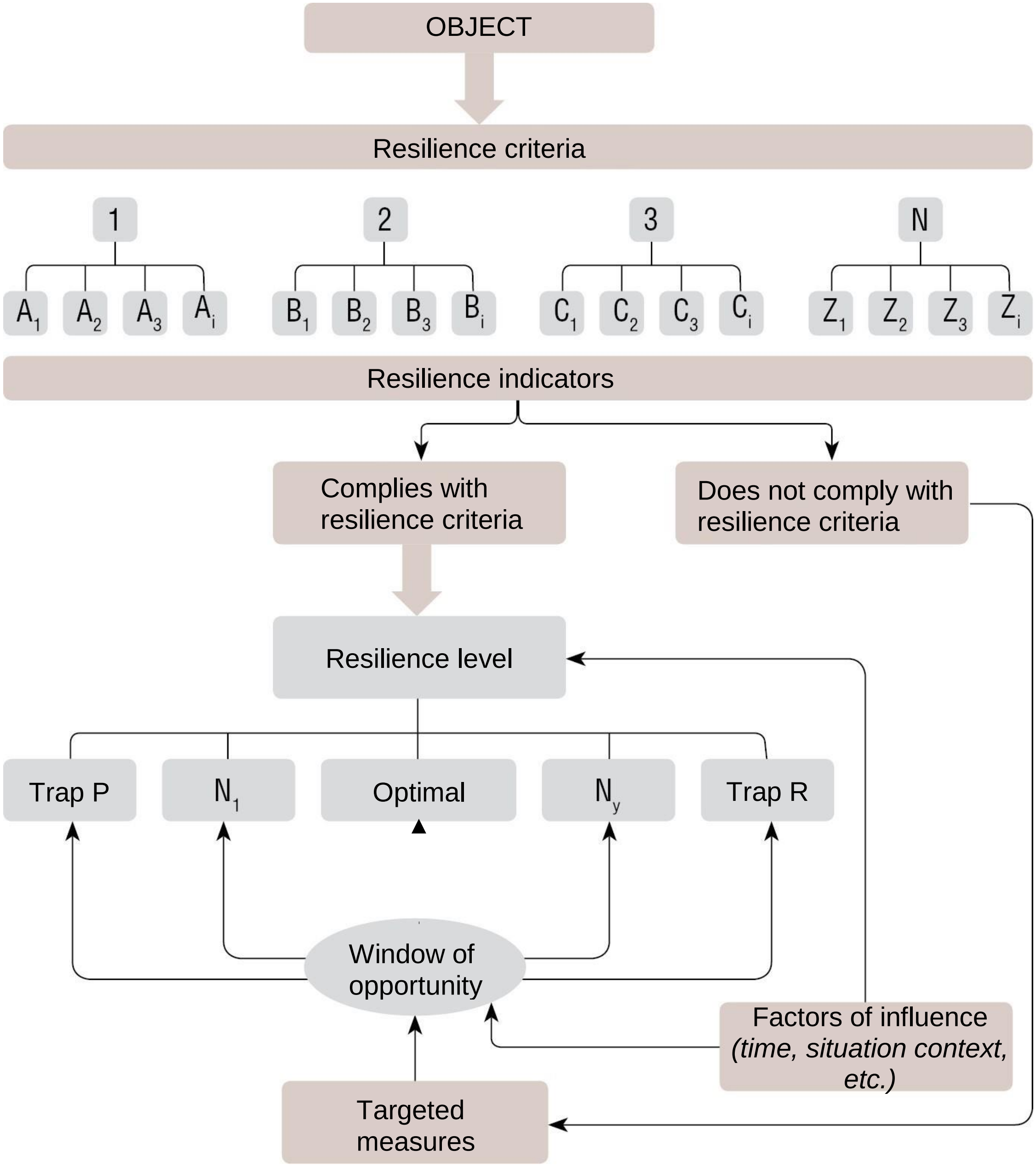


Fig. 1.4. General resilience management algorithm in the national resilience ensuring system

Source: developed by the author.

System capabilities that provide system resilience create a potential of the system allowing it to effectively respond to threats and destructive influences and adapt to a changing security environment. In the national resilience ensuring system, such potential forms a pool of human, logistical, financial, and natural resources and reserves of the state, purposeful activities of national resilience ensuring actors, organizational links, knowledge, and skills to respond to threats and crises.

So, we can offer the following definition of capabilities in the national resilience ensuring system: ***capabilities*** are a combination of all available resources, forces, and means of a state, society, community, or organization which determines their ability to effectively respond to threats and crises at all stages of the crisis cycle and adapt to the changing security environment (Reznikova & Voytovskyi, 2021).

The capability factor is important to provide national resilience.

Sufficiency of capabilities determines the reliability and redundancy of the national resilience ensuring system and contributes to its adaptability. The capability development level affects the effectiveness of responding to threats and crises and the crisis recovery rate. Insufficient or underdeveloped capabilities may make a state and society vulnerable. Therefore, the capability factor can strengthen or weaken national resilience by the relevant criteria of the system's state and system's functioning.

Vulnerability can be characterized as existing problems, defects, and deficiencies that cause or increase the susceptibility to disruption, systemic damage, and/or susceptibility to adverse effects of risks and threats (Reznikova & Voytovskyi, 2021).

According to Proag (2014), the vulnerability phenomenon implies the existence of a certain risk in combination with social and economic responsibility and the ability to cope with a hazard. The researcher argues that vulnerability is defined as the level to which a system, or part of it, may react adversely during the occurrence of a hazardous event.

Chandler (2012) emphasizes that vulnerabilities can be both the result of the system's inability to make the right choice and the product of certain external circumstances. So, the scientist points out that vulnerabilities constitute our "unfreedoms" or the restrictions, both material and ideological, that prevent us from being resilient. As examples of different vulnerability degrees, Chandler (2012) points out the following conditions of individuals: "at risk," "socially excluded," and "marginal;" of communities: "poor," "indigenous," or "environmentally threatened;" and of states: "failing," "failed," "fragile," "low income under stress," or "badly governed."

Summarizing the above, we can argue that *vulnerabilities not only exacerbate external threats but can also be a source of internal threats to the state and society, and therefore, timely detection and elimination of vulnerabilities is an important part of national resilience policy*.

1.3.5. Key Processes, Principles, and Mechanisms of Ensuring National Resilience

Based on the above regularities of ensuring national resilience and functioning of the relevant system, we can conclude that a significant part of the targeted actions of various actors falls on the *stage preceding the crisis or threat (pre-crisis)*. Preparations for a possible response to threats and crises are made, the necessary knowledge and skills are disseminated, reserves are formed, and vulnerabilities are identified during this period. We should note that the following crucial national resilience providing processes should be carried out at this stage with due account to the peculiarities of adaptive management:

- continuous security situation monitoring;
- risk assessment, identification of threats and vulnerabilities, assessment of capabilities and readiness of various actors to respond to threats and crises;
- preventing threats, minimizing destructive influences and possible impacts of threats and crises, eliminating reasons for conflict developments;
- providing readiness of public and local authorities, institutions, enterprises, organizations, communities, civil society, and population to respond to any threats and crises;

- planning measures and crisis management, including developing sectoral and organizational resilience plans, introducing universal concerted action protocols of response to threats and crises and recovery of the essential spheres of state and social life to a level not lower than pre-crisis;
- establishing effective coordination and strong interaction between national security and defense sector agencies and other state bodies, territorial communities, businesses, civil society, and the population in preventing, responding to, and recovering from threats and crises;
- acquiring and disseminating knowledge and skills necessary to ensure security and resilience;
- establishing and maintaining reliable communication channels between public agencies and civil society;
- development of international cooperation in the field of resilience.

Researchers identify various processes as key to providing national resilience. For example, Donno (2017) pointed out that the following processes are important:

- continuous risk management;
- emergency management and crisis communication;
- environmental and critical infrastructure protection;
- national security and anti-terrorism;
- informational transparency etc.

It should be noted that most of the above processes aim to provide the ***readiness*** of the state and society which means the ability to timely and effectively respond to threats and crises.

During a crisis or emergency, appropriate knowledge, skills, formed capabilities, plans, reserves, and well-established liaisons allow responding effectively to threats and reduce human, material, and financial losses caused by threats or crises of any nature and origin in order to provide continuous functioning of key areas and provision of essential services.

After a crisis, the recovery rate of the quality of life and conditions of the society and state at a level not lower than pre-crisis will indicate both how ready the state and society are and how national resilience complies with basic criteria.

Prolonged and exhausting recovery largely results from a lack of attention to pre-crisis measures.

Given that feedback is an important factor in complex systems' resilience (Ashby, 1960; Bertalanffy, 1968), we should emphasize that learning lessons is important to ensure national resilience. In particular, lessons learned improve the existing crisis management practices and use the obtained information in the next risk and consequences assessment cycle. However, it is important not to fall into the institutional and other traps mentioned above. In particular, while preparing strategic documents and contingency plans we need to keep in mind that in addition to risks known from experience new ones should be considered, especially risks called "black swans." They are very difficult to predict, but the materialization of such threats can significantly and suddenly change the security situation and simultaneously affect different areas. The rapid spread of COVID-19 all over the world is such an example. The question of risk assessment peculiarities and methodology will be covered in more detail in Chapter 2 of the monograph.

In view of the above, we can define the ***national resilience ensuring cycle*** as a sequence of actions of national resilience actors which allow to effectively counter threats of any origin and nature, adapt to changes in the security environment, and maintain continuous functioning of essential life spheres of the society and state before, during, and after a crisis in order to survive and develop (*Fig. 1.5*).

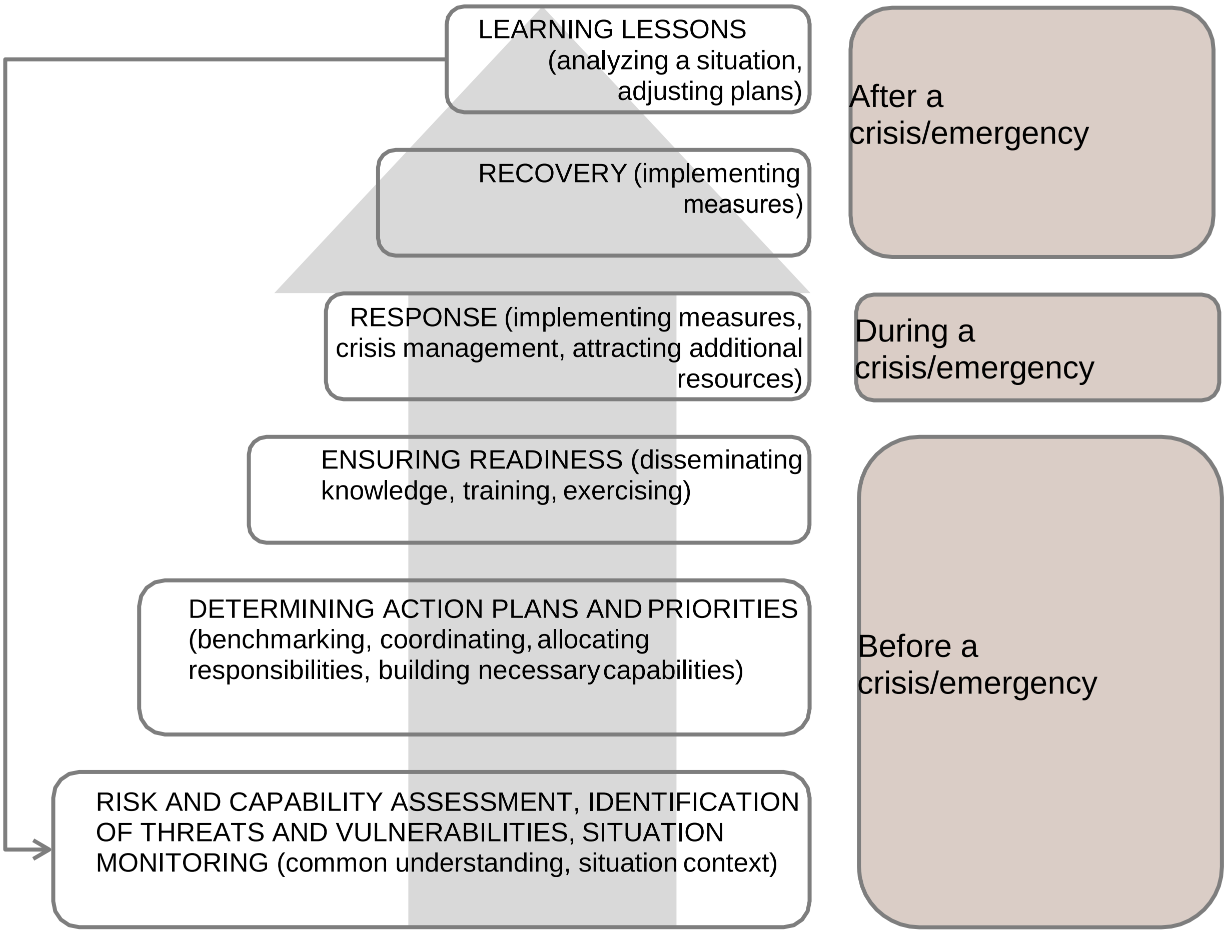

LEARNING LESSONS (analyzing a situation, adjusting plans)
RECOVERY (implementing measures)
RESPONSE (implementing measures, crisis management, attracting additional resources)
ENSURING READINESS (disseminating knowledge, training, exercising)
DETERMINING ACTION PLANS AND PRIORITIES (benchmarking, coordinating, allocating responsibilities, building necessary capabilities)
RISK AND CAPABILITY ASSESSMENT, IDENTIFICATION OF THREATS AND VULNERABILITIES, SITUATION MONITORING (common understanding, situation context)
After a crisis/emergency
During a crisis/emergency
Before a crisis/emergency

Fig. 1.5. National resilience ensuring cycle

Source: developed by the author.

Given that modern threats and responses are complex sets of links and relations, we can argue that ensuring national resilience is an open, constantly evolving, and adjusting process. This conclusion justifies the expediency of making national security and resilience policy more flexible through adaptive management.

Considering the content of the national resilience concept, it would be appropriate to define the following key organizational and functioning principles of the national resilience ensuring system:

comprehensiveness – taking coordinated measures against any threats and crises at all stages of the national resilience cycle;

inclusion (broad interaction) – implies that all involved actors continuously share necessary information, communicate with each other in different formats, jointly perform certain tasks within the determined responsibilities;

adaptability – the ability of the system to adapt (without significant loss of functionality) to new or crisis conditions, that have arisen under a threat or crisis, to ensure survival, evolution, the ability to transform negative results into positive ones, and to apply innovative solutions;

predictability – timely identification of threats and vulnerabilities and risk assessment;

reliability – implies that the system is fully operational and able to overcome failures that occur under the influence of threats and crises, and all the involved actors have sufficient and developed capabilities to respond to threats and crises;

awareness – implies that all the involved actors have the appropriate knowledge and practical skills to respond to threats and crises at any stage;

readiness – availability of action plans for a joint response to any threats; appropriate level of theoretical and practical training of all the involved actors in order to respond at all stages of the national resilience ensuring cycle;

mobility – the ability to quickly involve primary and backup forces, means, resources, and join efforts to achieve objectives under threat or crisis;

redundancy – additional capabilities of a system that can be used after primary ones fail, as well as alternative plans and development strategies;

continuity – implies that in crisis or under influence of a threat, the system continues to operate without significant loss of functionality, and all the involved actors are able to perform their basic functions;

subsidiarity – aims to allocate powers and responsibilities so that decisions on responding to threats and crises are made at the lowest possible level with coordination at the relevant higher level.

It would be reasonable to assume that key processes that must take place to ensure national resilience and organizational principles of the relevant system are crucial to forming national resilience ensuring mechanisms.

National resilience ensuring mechanisms are sets of decisions and measures that determine a sequence of certain processes and actions that meet general aims and functional principles of the national resilience ensuring system and are focused on achieving the determined resilience level and criteria by the state, society, and their individual components.

According to the content of the national resilience concept, it would be expedient to define the following *key objectives* to be solved by these mechanisms:

- adaptation of the national security policy and management system of the essential life support spheres of the state and society to uncertainty and rapid changes in the security environment;
- eradication of the causes that give rise to the vulnerability of the state and society;
- providing continuity of governance and critical financial and economic processes in the state, organizational resilience of state and local authorities, continuous functioning of the essential life support spheres of the state and society (primarily critical infrastructure) in normal mode, during and after crises;
- ensuring public resilience to destructive influences (including information);
- providing prompt restoration of the quality of life of the population and proper functioning of society and state after devastating impacts of threats and crises of any nature and origin to a level not lower than pre-crisis.

In general, national resilience ensuring mechanisms aim to achieve these objectives and have a common base, but they may have peculiar features depending on their scope of application (economic, environmental, or political) Thus, it is possible to distinguish universal and special national resilience ensuring mechanisms. *Universal mechanisms* determine the organization of cross-sectoral processes or certain types of activities that require the interaction of different national resilience actors. *Special* mechanisms are used in certain branches or spheres of activity with due account for their functional specifics and general approaches to providing national resilience.

In order to implement a systems approach to ensuring national resilience, the state must first form and implement universal mechanisms that will make the basis of the national resilience ensuring system. This will help introduce a common understanding of the aim and objectives in this area, eliminate duplication of functions, and use resources of the state and society efficiently.

However, this does not mean that special resilience mechanisms cannot be applied in different branches and areas until the relevant system is in place.

System resilience ensuring mechanisms may also differ depending on their purpose. In particular, Moench and Dixit (2007) notes that system resilience may form in two ways:

1) the direct strength of structures or institutions when placed under pressure (hard resilience); and
2) the ability of systems to absorb and recover from the impact of disruptive events without fundamental changes in function or structure (soft resilience).

Extrapolating this conclusion to providing national resilience, we can argue that national resilience ensuring mechanisms can form in two main directions, namely:

- strengthening state and society institutions and capabilities in counteracting modern threats and dangers, which implies, in particular, timely detection and elimination of vulnerabilities;
- introducing new processes and sets of measures (organizational, technical, and economic) that will enable the state and society to adapt to the continuous effects of a wide range of threats and disruptive influences.

Any combination of appropriate measures could be used in practice. In particular, the first type of national resilience ensuring mechanisms include reforming and developing the national defense and security sector, revising security strategies and doctrines, forming joint security capabilities of communities and mobilization reserves, developing early warning systems and the state situation centers network, continuous exercises and training both for state servants and the population regarding the nature of certain threats and procedures in case they escalate.

It would be appropriate to highlight the following most important groups of the second type of national resilience ensuring mechanisms:

- providing governance continuity, including the guaranteed succession of power, strengthening coordination between authorized state bodies, forging communication between them and non-governmental actors (including through forming targeted interagency groups, partnerships, and permanent networks);
- ensuring continuity of critical services to the population (including creating a critical infrastructure protection system, sectoral action plans, and concerted action protocols for crises response);
- creating a multi-level system to assess risks and capabilities and identify threats and vulnerabilities;
- forging stable two-way communication channels between the authorized state and local authorities with the population.

It should be added that such activities as improving legislation (including strategic planning and crisis management principles), coordinating forces and means, and follow-up monitoring are cross-cutting and may be part of both the first and the second type mechanisms.

Given that modern hazards can threaten not only a state but also a society, individual organizations, enterprises, and people, the resilience ensuring mechanisms can be both complex (operate at the state level) and individual –

implemented at the level of individual actors (institutions, organizations, subsystems, and communities).

Summarizing the above, we can state that it is very important to define priorities in forming and applying certain national resilience ensuring mechanisms and their settings (in particular, establishing an acceptable risk level and optimal resilience level of various objects under certain conditions) in order to form national security and resilience policy. Its development and implementation features will be described in the following chapters of the monograph.

Conclusions to Chapter 1

As a scientific direction, national resilience studies have formed as a result of the development and mutual enrichment of various scientific disciplines: primarily complex systems studies, sustainable development studies, and security studies. Science and technology advancements, new emerging threats, and expanding traditional ones point out that the national security ensuring system is inconsistent with new conditions, so new conceptual approaches and areas for improvement should be found.

Although the issue of national resilience formation is actively included in the agenda of many states and international organizations, we can state that there are still no established definitions of this term, its generally accepted criteria, methods of national resilience assessment, and requirements for building a national resilience system. Different interpretations of the resilience concept in national security cause different approaches to public policy in this area. Such an ambiguous situation leads to substitution of notions when under the pretext of strengthening national resilience, some experts and officials propose inconsistent excursive measures with insignificant overall effectiveness and high resource consumption.

Given that the current security environment is becoming more aggressive towards the state and society with more destructive impacts, it seems justified to establish an additional comprehensive mechanism aimed at strengthening the resilience of these system-forming objects to ensure their security and further development in conditions of uncertainty. The national resilience ensuring system is such a comprehensive mechanism that it should be practically formed with due account for fundamentally important theoretical conclusions and regularities within the national resilience concept.

Among important theoretical conclusions, we would emphasize that the state and society are complex systems, and their components may be differently affected by different threats. Besides, passive security objects can turn into actors that self-ensure their resilience, and the increasing total number of resilient objects and actors can strengthen the overall national resilience. It should be noted that in order to practically achieve this, citizens need to change their paradigm of thinking and form a more active and responsible stance on current and future consequences of their actions or inaction, especially in security.

According to the formulated theoretical foundations for building national resilience ensuring system, not only the characteristics of its systemic elements and the links between them but also defining its mission, aim, operation principles, key processes, details of applying universal and special mechanisms, nature of interaction with other systems, and influences from the internal and external environment are important. The key processes that should take place within the national resilience ensuring cycle and the formulated principles of such activities are crucial to forming state policy in national security and resilience, including the prioritization of the relevant mechanisms and measures.

After a comparative analysis of the essence and fundamentals on which the national security ensuring system and the national resilience ensuring system are formed, we may see their compatibility and possible synergistic effect from their interaction. It is justified to separate the national security ensuring system and the national resilience ensuring system for research purposes. But practically, keeping a separate national resilience ensuring system to operate in parallel with the existing national security ensuring system can be too burdensome for the state. Given the limited resources and common characteristics of both systems, it would be more appropriate to say that resilience principles and the relevant mechanisms should be implemented in the national security field. A comprehensive national security and resilience ensuring system implemented in such a way would significantly increase the effectiveness of countering modern threats and destructive influences in uncertain and changing security environment.

Close links and mutual influence between national resilience objects, actors, other systems, and the external environment result in the complex nature of measures aimed at providing national resilience to cover political, social, psychological, and other aspects.

A comprehensive state policy in national security and resilience should be elaborated and implemented with due account for the content of the national resilience concept and the relevant regularities. In particular, it is important to identify which elements and characteristics of key objects and their components must remain unchanged in order to provide their integrity and basic functions and which can be correlated to strengthen national resilience. Relevant public policy should also take into account the adaptive behavior of complex social systems and their ability to self-organize and self-govern, how the general situation context and time influence the effectiveness of national resilience ensuring measures, and what resilience, institutional and other traps exist.

In general, in a changing security environment, state policy in national security and resilience should be developed and implemented with sufficient flexibility and based on adaptive management due to the fact that ensuring national resilience is an open, constantly evolving, and changing process.

As an adaptive management component, national resilience assessments should be performed regularly while formulating and implementing the state resilience policy to provide information necessary to identify and adjust priorities and measures that should be taken in the state and society to achieve a certain resilience level. Such assessment is a complex process. It is based on the use of criteria of resilience state and resilience functioning of the state and society and their subsystems, analysis of indicators developed with due account for the specifics of different spheres of social relations, as well as resilience levels of various objects that may fluctuate within a certain range and have to take situation context and other influencing factors into account.

There is also one more important theoretical conclusion of high practical importance: greater predictability of changes in a complex system may result not only from analysis of the environment, which is a source of destructive influences, but also from the active influence of the system on such an environment. In the context of providing national resilience, this emphasizes the need to transfer from reactivity to greater proactivity in formulating and implementing state policy measures in this field.

The above study reached theoretical conclusions about the features and regularities of the establishment and functioning of the national resilience ensuring system. These conclusions are crucial to forming the model of this system and to considering the peculiarities of each state and the development and implementation of national security and resilience policy in general.

Chapter 2
METHODOLOGICAL TOOLS FOR ENSURING NATIONAL RESILIENCE

In order to develop and implement any national resilience ensuring mechanisms and measures, we need to use appropriate methodological tools allowing us to streamline these activities and determine priority aims and objectives. As building national resilience is a fairly new task for the state and society, it is especially important to determine conceptual approaches to choosing a national resilience ensuring model and key system parameters and forming appropriate state policy with due account for the content and regularities of the national resilience concept.

2.1. Peculiarities of Development and Implementation of State Policy in National Resilience

2.1.1. The Role of the State in Providing National Resilience

As already mentioned, a national resilience ensuring system differs from a national security ensuring system. In particular, they have different principles of interaction between their actors and establishing system links. It is important to find out how the role and functions of the state as one of the key actors differ in both cases (Reznikova, 2018d).

Discussion about the role of the state in the social relations system is one of the main topics of political science. Today, this issue is becoming quite relevant because changes that take place in the modern world lead to the disruption of many existing ties, increasing uncertainty, and vulnerability for most social relations actors. The liberal political doctrine, which now dominates in most countries, is being revised to see if it is still in line with the new development conditions.

One of the key issues in the modern national resilience discourse is the impact of this concept on state-building processes and policy-making in national security and governance. Bourbeau (2013), Joseph (2013), Zebrowski (2013), Chandler (2014), and other scholars note that today, under the influence of changes in the world, some shifts in the social relations system are coupled with resilience-building at the level of both nation-states and international organizations. While Chandler (2014) considers national resilience to be a manifestation of a new post-liberal political paradigm, Joseph (2013) disagrees, saying that it is an embedded and currently developing feature of neoliberalism.

Such discussions reflect the change in social relations format since World War II. It is influenced by globalization, entry of new players into the international arena, etc. In particular, the role of the state in providing national security is being reviewed. The need to build national resilience in response to emerging threats and growing uncertainty in the world also influences state policy-making.

Chandler (2012) points out that the human security concept has changed the traditional liberal understanding of national security and sovereignty. Priorities have shifted: first of all, people, not territories, should be secure, and investments must flow into sustainable human development, not in armaments. Chandler (2012) argues that all this, as well as the expansion of rights and opportunities, is shifting focus towards understanding security according to the bottom-up principle. Security institutions become “de-liberalized”, and we see a departure from the model of social relations, which envisaged mandatory intervention of a state or international institutions to correct any problematic results upon their occurrence. According to the scholar, this allows us to consider the human security concept from the perspective of the resilience and decentralization of power (Chandler, 2012).

Zebrowski (2013) emphasizes that national resilience enables to enhance national security and governance. Instead of traditional approaches and management methods, these systems should strengthen such “embedded” features that will allow them to adapt to new conditions and dangers. As the complex systems theory founders conclude, such systems tend to keep their structure and basic functions stable (Ackoff, 1971; Ashby, 1960; Bertalanffy, 1968; Bogdanov, 2003). In the context of providing national resilience, this means that the state and society have a certain resilience and self-organization potential, which can be managed and strengthened through the relevant state policy measures which envisage, inter alia, developing and sophisticating links between various actors and objects.

The application of the monocentric principle in the national resilience ensuring system has certain peculiarities. Bogdanov (2003) found that a system is much more stable if its elements gravitate to one center, and in the case of complex systems – to one higher common center, wherein each group of elements connects to the nearest center. If several coordination centers operate simultaneously at the same level, contradictions, disorganization, and imbalance of the system increase. At the same time, Bogdanov (2003) notes that the other type of system organization, which gives its elements greater autonomy, although less resilient to external influences, allows the system components to develop more freely and gain additional development potential from the environment.

As noted in Chapter 1 of this monograph, the system links in national security form according to the “top-down” principle while in national resilience they form according to the “bottom-up” principle. Based on the conclusions of the above-mentioned researchers, we can say that *it is essential to find the optimal balance between centralization and decentralization of governance processes, as well as between state governance and local self-governance (including in security) to form a modern organizational model of ensuring* *national security and resilience*. These processes are schematically shown in *Fig. 2.1*.

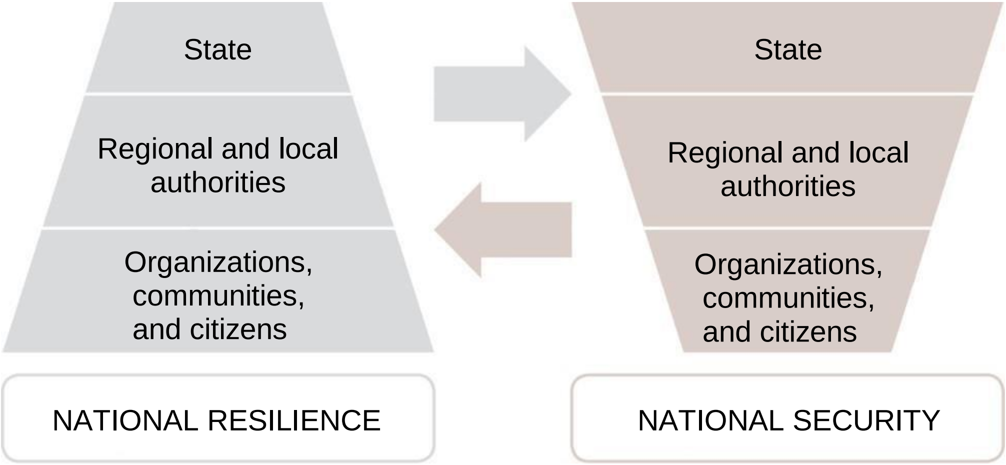

State
Regional and local authorities
Organizations, communities, and citizens
NATIONAL RESILIENCE
State
Regional and local authorities
Organizations, communities, and citizens
NATIONAL SECURITY

Fig. 2.1. Balancing centralization and decentralization governance principles in a comprehensive system of ensuring national security and resilience
Source: developed by the author.

There is an ongoing debate among modern scholars about how the role of the state in providing national security should change in current conditions. Zebrowski (2013), and Joseph (2013) believe that if the resilience concept is implemented in national security, a special form of governance with the reduced role of the state is formed, which corresponds to the ideas of neoliberalism. At the same time, Evans and Reid (2015) believe that the conceptualization of national resilience leads to irresponsibility of governance, as it shifts much of the responsibility for national security to the people.

In modern conditions, the state is the main contributor to security at the national level. It retains its monopoly on the right to use force and has the relevant capabilities (Reznikova, 2018b). This corresponds to the classical national security approach formulated by M. Weber at the beginning of the previous century (Weber, 1919, as cited in Waters, 2015). However, we should take into account that since then, the world has changed significantly, globalization processes have become more dynamic, technologies have developed, and new threats have emerged.

In particular, a distinctive feature of currently widespread hybrid threats is that they are difficult to identify (especially at the initial stage), are long-term, and are often initiated by non-state actors. A hybrid war aims not to establish control over a certain territory, but to destabilize the state and society under aggression to weaken their ability to protect national interests and values. Hybrid threats are difficult to predict and prevent. As it is almost impossible to completely overcome such threats, crisis management, preparedness to respond to threats and crises, and creation of new interaction formats, in which it is possible to minimize the adverse effects of threats of different nature and origin, are becoming increasingly important. So, there is a demand for new functions of national security, which would meet the essential characteristics of the resilience concept in the field of national security. Here we should also mention some need to redistribute powers and expand the role and scope of responsibility of the state, local authorities, and non-state sector, including civil society, in counteracting a wide range of threats.

Fjäder (2014) notes that the national resilience concept changes the traditional role of the state in national security due to the more complex nature of social relations and growing uncertainty in the modern world. According to Joseph (2013), the world is gradually moving away from strong ties based on classes and national or social identities in favor of individualism. Modern society can be considered as a set of "individualized consumer-citizens with their own life-pursuits". A characteristic feature of modern times is that citizens are less and less actively involved in political life (participation in elections, membership in political parties, etc.) in many countries (Joseph, 2013).

Therefore, *a rigid hierarchical governance model cannot be very successful in addressing complex issues of providing national security in modern conditions*.

In this context, it is particularly important to form a set of resilient objects and actors able to effectively overcome threats (Reznikova, 2018a). It is about how to apply resilience ensuring mechanisms for the state, society, organizations, enterprises, etc., as well as create new interaction formats for various actors in this field. Besides, self-organization and self-governance as specific manifestations of resilience should also be considered. We will analyze this issue more thoroughly below.

Practical implementation of the national resilience concept does not mean the state's irresponsibility or significantly reducing its powers in providing national security. First of all, it means redistribution of powers between the state and other actors that ensure national resilience. By partly transferring national resilience ensuring functions to lower-level actors, the state should establish comfortable conditions and clear rules for such activities and the development of relevant capabilities, as well as foster broad interaction and coordination (Reznikova, 2018a).

Chandler (2012) emphasizes that the purposeful transfer of security powers implies that the state delegates them to actors that are capable to secure themselves and, therefore, have the capabilities necessary to adapt to potential threats.

According to the Secretary-General of the UN (2013), providing security is one of the key state functions. However, the increasing variety of factors that affect the modern security environment suggests that the security of the state and the state of security (of individuals and communities) are mutually interdependent: when populations are not secure, neither is the State (Secretary-General of the UN, 2013). This conclusion became especially relevant for Ukraine with the beginning of the hybrid aggression of the Russian Federation, as non-military measures against the Ukrainian population (propaganda, dissemination of disinformation, incitement to ethnic and interfaith hatred, etc.) became the aggressor's main weapon.

The synergetic effect of the interaction between the national security ensuring system and the national resilience ensuring system reveals primarily in objects and actors acquiring new properties that allow them countering threats and adapting to change more effectively. This requires improving their interaction management. Taking into account the above, we can conclude that state policy-making in national security and resilience should be comprehensive. This is due to the fact that, on the one hand, such a policy should aim to provide the resilience of the state itself, and on the other – to create conditions necessary to strengthen the resilience of other actors and introduce effective mechanisms for their cooperation. This requires the optimal balancing of the relevant objectives within limited resources.

According to Edwards (2009), the role of the state in shaping the resilience of other actors will always be limited. However, from this scholar’s point of view, it is expedient for the state to focus more on creating the necessary conditions by arranging interaction between actors, expanding their capabilities, ensuring interest in the outcomes, and conducting appropriate training. Bohle, Etzold and Keck (2009) draw attention to the important role of social actors and their agents in providing national resilience (especially if we consider resilience as the ability to support the protective capabilities of vulnerable life support systems), strengthening the adaptive capacities of people and their institutions, or generating innovation and learning that allow for resilient transformations. According to researchers, this resilience perspective aims to regulate entitlements, capabilities, freedoms, and choices based on the principles of justice, fairness, and equality (Bohle, Etzold & Keck, 2009).

As the key actor, the state plays an essential role in building national resilience in developing countries, especially in transition and in conditions when security culture has not yet matured in a society. Analysis of international experience also shows the growing role of other actors in providing national resilience. They not only perform their certain delegated functions but also actively participate in many processes in this field.

At the same time, the role of the state in providing national resilience is to a certain extent deterrent, as the state should act through clearly defined bureaucratic procedures and specially established state institutions. The need to comply with the established rules and restrictions makes the system less flexible and adaptable and increases the risk of managerial errors. Under modern conditions, it is expedient to strengthen individual adaptability, readiness to respond, and responsibility of other actors (local authorities, communities, organizations, individuals, etc.) in providing national security and resilience.

Other problems may arise while relations between the state and other national resilience actors form. Fjäder (2014) highlights a dilemma caused by the fact that the state sets certain national security and resilience standards and rules, which require all participants to perform certain actions, including those that require spending their own resources, including financial ones. However, private owners are primarily interested in increasing their investment profitability, and, therefore, business may not be interested to invest in national security and resilience. This is the most problematic issue in security and resilience of critical infrastructure, which increasingly belongs to private owners according to world practice. In line with Fjäder (2014), it is not the best policy choice to nationalize such facilities or impose severe restrictions on their owners to solve this problem. Therefore, the researcher believes that the issue of amending the social contract regarding the risk management principles is ripe.

In addition to a possible conflict of interest in the field of national resilience, other problems in social relations may arise. In particular, among the barriers to national resilience-building, Chandler (2012) singles out stereotyped thinking based on past experience, as well as certain cultural and social values that remain unchanged and limit the space for maneuver and adaptation.

In the context of providing national resilience, governance should primarily encourage various actors to take action to strengthen their own capabilities, create effective organizational formats for inclusive interaction and strong motivation for such activities. The national resilience organizational support model can base both on the division of responsibilities established by the legislation and by contract. The latter is extremely important for fostering public-private partnerships, including determining concerted action in crises. Besides, each of the national resilience providers should be aware not only of the long-term benefits of cooperation in this area but also of possible losses from a crisis and the procedure for full or partial compensation.

Summarizing the above, we should note that within the traditional national security ensuring system, the state performs basic functions, and other actors (citizens, civil society, institutions, organizations, enterprises, etc.) are involved in performing certain functions as appropriate (for example, in the case of mobilization or civil control). Certain powers are being redistributed within the national resilience ensuring system: non-state actors are exercising more powers on a permanent basis (in particular, providing readiness to respond to threats and crises, building joint capabilities, etc.). At the same time, the coordinating and controlling functions of the state are strengthening. Such changes should be reflected while the state forms and implements its national security and resilience policy.

2.1.2. Self-Organization and Self-Governance Potential in Strengthening Resilience

Taking into account that complex systems are capable to self-organize and self-govern, which allows them to counteract adverse impacts and regain equilibrium, it is important to recognize that not all the systems are equally capable of doing so.

According to Kaufmann (2013), the most striking examples of systems with a high capability for self-organization and self-governance are societal networks that dominate in the age of informationalism. They are able to not only adapt to changes in the environment but also shape it by their actions. According to the scholar, flexibility of the decentralized structure and informal network connections provide space for maneuver in the event of a crisis, but needs timely information about changes (Kaufmann, 2013).

However, it is not only Internet-based networks that are capable to self-organize. A volunteer movement that was quickly formed in Ukraine in early 2014 is a striking example of this. The movement provided significant assistance to the Armed Forces of Ukraine and other government structures in providing national security and defense against hybrid aggression by the Russian Federation. *Spontaneous self-organization* mechanisms were triggered in this way, thus showing the resilience potential of the state and society.

According to Kaufmann (2013), *resilience governance* is intended to streamline system self-organization processes as a set of measures that are planned and prepared through training and implemented during crises. The scholar proposes to coordinate and control the networks through the idea of common values, goals, and response protocols. The latter should be emergent, highly flexible, and inclusive rather than exclusive (Kaufmann, 2013). So, this is the way a *regulated (controlled) self-organization* takes place.

An important direction of state policy in national security and resilience is determining measures aimed to assess the self-organization potential of society and manage it. It is based on findings of security environment analysis, assessments of risks and their possible impacts, identification of threats, estimations of capabilities needed to counter threats, and elaboration of concerted action protocols in case of threat or crisis, planning of response and recovery after crises, and fostering communication between different actors and their effective interaction, etc.

Territorial communities, institutions, organizations, enterprises, public associations, families, etc. have self-organization and self-governance potential. In the context of providing national resilience, the main ways to establish control over self-organization and self-governance processes are to clearly allocate roles and responsibilities among all actors, disseminate the necessary knowledge and skills to respond to threats and crises, form appropriate rules of interaction between actors, etc. Hence, the state has the following important sectors of activity in this area: crisis management, arranging crisis exercises and training, establishing reliable communication channels, and proper legal support of national resilience management processes. General recommendations on how to form organizational and community resilience could be found, in particular, in a range of international standards (ISO 2017a, 2018b, 2020). National resilience actors should develop specific measures and plans to strengthen general and specified resilience with due account for these standards.

According to the prevailing world practice, the government shall determine long-term objectives in providing national resilience. In the context of building the resilience of society to various threats and crises, such objectives are, among others: to prevent panic in a crisis and join capabilities of citizens and authorized government agencies in recovery. To practically achieve this aim, it is necessary to analyze processes that affect the resilience of society and communities to various threats.

From the standpoint of Pollack and Wood (2010), to form social resilience, it is important to consider not only the direct consequences of threats (destruction, casualties, etc.) but also behavioral, psychological, social, and political aspects. In particular, the scholars take forming public resilience to the terrorist threat as an example and point out several fundamentally important elements for developers of the relevant state policy measures to focus on:

1) the public's sense of comprehension (which moderates fear of the unknown);
2) the public's sense of control (which moderates fear of perceived threat); and
3) social resources (which moderate fear and hinder panic, creates social ties, and social capital).

It should be noted that the recommendations of Pollack and Wood (2010) may be expanded to the formation of social resilience to other threats and crises because a terrorist threat is just a one of them, that cannot be predicted or completely overcome. It remains relevant for all states, as a terrorist threat is based on the tactics which can be used to achieve different aims by different actors and which essentially cannot be eliminated. According to recent experience, not only weak states but also those with developed counter-terrorism systems (in particular, France, Belgium, and Germany) were among the countries that suffered terrorist attacks. Thus, it will be much more efficient to respond to such threats at different stages on the basis of national resilience principles (Reznikova, Misiura, Driomov & Voytovskyi, 2017).

According to Pollack and Wood (2010), society needs to perceive a threat as understandable and controllable (even if this feeling is illusory). This reduces public fear, allows avoiding panic and acting in concert, and relieves the impact of the threat, which may sometimes include loss of public confidence in government institutions, increased violence, and other destructive processes in society. Continuous raising public awareness is particularly important here in order to form a public sense of safety and understanding of the plan of actions in the case a particular threat increases. As these researchers conclude, the public is willing to support more regulatory controls and security measures in the cases of dread of unknown or uncontrolled threats (Pollack & Wood, 2010).

At the same time, Kaufmann (2013) argues that the self-organization and self-governance potential of the society can demonstrate itself in crises spontaneously. This is evidenced by the example of Ukraine, when at the beginning of the aggression by the Russian Federation in 2014, the civil society was the major driving force of resistance, despite the lack of relevant experience and practice in combating large-scale threats, including hybrid. In other words, people quickly united around the ideas of defending national sovereignty, freedom, and mutual assistance, and this was their conscious choice. For the self-organization and self-governance processes to be controlled and purposeful in crises, the authorized state bodies need to organize and conduct the necessary training and exercises in advance and form and test concerted action protocols. According to Kaufmann (2013), such training aims to form interagency coordination and decision-making culture and optimize strategic crisis management.

Regular exercises allow local communities to develop necessary response skills to prepare them for crises. A community should respond to a crisis within the established national rules and standards. Given the above, one of the objectives of state policy in national security and resilience should be to involve the public in the formation and implementation of such policies as active, self-governing, informed, free, and responsible citizens who care about their safety and security.

Thus, *efficient state policy can strengthen the self-organizing potential of the society, communities, and organizations, as well as ensure its targeted application*.

2.1.3. Problems of Planning Under Uncertainty

According to generally accepted norms and rules, the practical implementation of the aims and objectives in providing national resilience should be based on the state's strategic and program documents, especially in the field of national security (Reznikova, 2018f). However, planning under uncertainty is extremely difficult. It becomes very difficult to determine specific long-term benchmarks, rather, only development vectors can be established. This foregrounds the problem of improving long-, medium- and short-term planning mechanisms, which requires proper scientific support to solve.

Given the above expediency of adaptive management in national resilience, planning relevant state policy measures in modern conditions should also be flexible and envisage regular reviews and updates of plans based on monitoring and analysis of security trends and key system parameters. In particular, the development of methodological principles in the field of strategic planning and management, the study of world best practices, and lessons learned help states formulate security strategies that meet modern challenges and requirements (Reznikova, 2020e).

Eisenkot and Siboni (2019) note that providing national security depends on the existence of a national strategy containing political, military, economic, and behavioral sub-strategies, as well as those related to social, demographic, and various other issues.

Classical approaches to *strategic planning* in defense and corporate management are now actively used in national security and remain relevant. The appropriate issues are covered in the works of famous scholars (in particular, I. Ansoff, H. Bandhold, P. Dixon, G. Kahn, M. Lindgen, G. Minzberg, J. Ringland, J. Steiner, and P. Schwartz), as well as Ukrainian scientists (i.e., V. Gorbulin, A. Kaczynski, G. Sytnyk, etc.).

According to the classical conceptual approach, such strategic documents should determine the desired model of state development, which guarantees the preservation of state sovereignty, territorial integrity, respect for human rights and liberties; promotes economic and cultural prosperity of the nation, international cooperation, etc. To this end, the long-term objectives of the state and society, ways to achieve them, and necessary resources should be determined based on the analysis of the global security environment and a situation in a country with the use of different forecasting methods.

One of the national security strategic planning features is that the resulting political, economic, informational, security, and other capabilities, as well as forces and means, can be used in peacetime, in wartime, or in crises to perform socially important tasks. According to Sytnyk (2010), the development of the National Security Strategy is considered as an art and as a science of creating and using state’s political, economic and information capabilities, as well as its armed forces in peacetime and wartime to implement national tasks.

Researchers point to the importance of distinguishing between strategic planning and strategic management. As Gorbulin and Kachynskyi (2010) conclude, strategic planning is a detailed description of the aim, objectives and a set of measures to implement the fundamental aims of the national security strategy. Strategic management is a governance function of managing the fundamental aims of the National Security Strategy and its implementation (Gorbulin & Kachynskyi, 2010). At the same time, most scholars agree that the national security strategy is a nationwide undetailed master action plan – a set of rules to achieve long-term goals in providing security and development of the state according to the determined national interests. In addition, Bucher (2009) points out that security strategy is important to integrate and coordinate various national security actors.

Eisenkot and Siboni (2019) note that National Security Strategy should focus on the following areas:

- the national and security interests whose preservation is critical to the existence, character, and values of the state;
- national security needs over the long term;
- national security objectives as derivatives of the defined interests;
- national strength that allows the state to independently confront national security risks of any type or scope (political, military, economic, demographic, social, etc.);
- military power that provides the capacity to defend the state’s sovereignty and territorial integrity, delivers safety to the state’s inhabitants, and prevents military threat to the state’s development and sovereign rights;
- economic, social, political, and demographic infrastructure that are capable of ensuring critical national and security interests for many years to come.

While developing a national security strategy, it is important to analyze the security environment in order to identify current and future challenges and threats, as well as global, regional, and national development trends.

In current conditions, national security *strategic management* is becoming increasingly important. Tama (2016) notes that the variable and unpredictable global security environment inherent in the modern world is becoming more and more challenging for national security strategic planning and increases requirements for arrangements of this process.

Development and implementation of a comprehensive state policy in national security and resilience enable, on the one hand, to make the state security policy more flexible and adaptable to rapid security environment changes, and on the other – to ensure that the state and society are properly prepared to respond to a wide range of threats, including hybrid. For example, the United Kingdom and the Netherlands' national security strategies have been formulated on this basis for a long time. Innovative solutions of these countries with due account for modern security environment features are actively studied and disseminated around the world (Caudle & Spiegeleire, 2010). Strategies developed on this basis are the foundation to elaborate sectoral, facility-based, and other plans for crisis preparedness and post-crisis recovery.

As we need to define aims and objectives for strengthening national resilience in modern conditions, it is expedient to explore what changes should occur during the preparation of state strategic and program documents, in particular the national security strategy. Donno (2017) notes that the resilience of a state implies not only its ability to deal with chronic stress and unexpected crises but also the ability to prevent and manage risks in a rapidly changing security environment. The researcher argues that the ability of a state to arrange close ties between different actors through the allocation of roles and enshrining them in law, as well as the development of long-term goals and action plans, is important in national resilience-building. It is essentially a matter of improving the processes of shaping the state's security policy and comprehensive national security and resilience ensuring system on the basis of participatory cooperation.

According to Van Gigch (1981a), the main problems indicating that system operation needs improvements are that this system:

- does not meet the assigned aims;
- does not provide expected results;
- does not work as expected.

The scientist concludes that after the main problem has been identified, it is necessary to determine objectives to solve it (Van Gigch, 1981a).

As already mentioned, the classical national security ensuring system is gradually losing its effectiveness in the face of current significant changes in the global security environment. It does not fully comply with predetermined aims, as it cannot guarantee full protection against all threats and hazards. Besides, it is becoming increasingly difficult to predict threats, especially hybrid ones. Although certain national security ensuring mechanisms remain fairly reliable, an issue to supplement them with other mechanisms, more effective under uncertainty, has arisen. This indicates the need to improve the national security ensuring system by combining it with the national resilience ensuring system. The relevant changes should be reflected in state strategic and program documents.

Based on the essential characteristics of the national resilience concept, presented in Chapter 1 of this monograph, we can determine a set of new objectives, which should be addressed, inter alia, by national security strategic and program documents in modern conditions. Among these objectives are the following:

- implementing an integrated approach to countering a wide range of threats at different stages;
- establishing effective cooperation between public authorities (both from the security and defense sector and other sectors), communities, businesses, and

the population to prevent and respond to threats and recover from their impacts, as well as to coordinate such activities;

- introducing common approaches to risk and changes management and identification of threats and vulnerabilities;
- establishing effective crisis management;
- providing continuity of the public administration process and providing essential services to the population and key business processes;
- ensuring the readiness of various actors to respond to any threats and crises and their ability to resist adverse influences;
- forming public security culture;
- ensuring high awareness among officials and citizens about the nature and possible effects of threats, as well as the plan of actions in case of crisis;
- fostering stable two-way channels of communication between authorized state and local authorities and the population, businesses, etc.

Solving these problems helps create (or strengthen) the necessary capabilities and builds the ability of society and the state to resist a wide range of threats, minimize vulnerabilities, adapt to security environment changes, function continuously even during crises, and recover quickly after a crisis to an optimum equilibrium on a previous or new level.

It should be noted that if a state has a scientifically approved security strategy, there is no guarantee for it to practically achieve the objectives and results determined in this document. Implementation of state strategic planning documents is influenced by many factors: political, resource, information, organizational, etc. The development of updated state strategic and program documents on national security and resilience is just the first step. Perhaps the most important is practical implementation of state-determined priorities and national resilience ensuring mechanisms, which implies adjusting day-to-day activities of state and local authorities, as well as forming public unity, trust, leadership, and security culture.

It is especially worth noting that in modern conditions, it is no less important to improve *crisis planning* than strategic planning. This follows from the complex nature of most modern threats and their possible large-scale cascading impacts. With this in mind, crisis planning should be based on participatory cooperation and public-private partnerships.

2.2. Forming a National Resilience Ensuring Model on the Basis of Systems Approach

2.2.1. Peculiarities of Selecting Key Parameters of a National Resilience Ensuring Model

One of the key issues in forming a national security and resilience policy is selecting a *national resilience ensuring model*, which determines the way to organize the national resilience ensuring system which best meets the needs of the state and its society. First of all, this implies determining aims, priorities, peculiarities of system links, and a specific set of national resilience ensuring mechanisms – i.e., key parameters to organize a national resilience ensuring system. According to Van Gigch (1981a), it is expedient to use a *systems approach* to analyze system that has a specific aim and is created by people to meet their needs. It allows us to consider the system as a whole, which helps provide the highest efficiency of the system despite contradictions among its components.

Since ensuring national resilience can be considered a type of management activity with its characteristic features, it is expedient to apply a systems approach from the complex systems management perspective to determine this system’s organizational model. Here, Van Gigch (1981a) recommends paying special attention to:

- determining the system scope and the nature of the system environment;
- identifying objectives of system operation;
- identifying the system's elements and structure;
- describing system management.

Chapter 1 of the monograph contains a general description of the national resilience ensuring system, its environment, elements, and system links. It is also proved that providing national resilience should comply with adaptive management principles, including ensuring targeted self-governance of individual subsystems. The effective functioning of this system largely depends on whether the regularities inherent in the national resilience concept have been taken into account in its design. In particular, it is necessary to take into account a range of rules that determine the purposeful behavior of complex systems while forming the national ensuring model and its basic parameters. Based on Van Gigch`s conclusions on the signs of system purposeful behavior we can highlight the following basic features of national resilience management:

- the system interacts with the environment;
- signals coming from the environment show whether the chosen behavior contributes to the achievement of the determined objectives;
- a course of actions should be chosen among several others;
- the final result depends on the chosen behavior;
- it is necessary to distinguish between sufficient and necessary conditions: sufficient conditions allow for predicting events while necessary conditions allow for determining the characteristics of the elements involved in the implementation of the event (Van Gigch, 1981a).

According to international experience, each state determines its national resilience ensuring model individually, with due account for its national interests and organizational features of the state power, as well as its security environment, membership in international organizations and alliances, etc.

(Reznikova, 2020c). Appropriate organizational and legal support systems, as well as specific resilience ensuring mechanisms, are formed within the model chosen by the state. As noted above, currently there are no uniform national resilience ensuring standards in the world, so the organization of a national resilience ensuring system, as well as mechanisms and priorities in this area, may vary from country to country. Practices quite effective in a number of countries may not meet the conditions and needs of others. This will be described in detail in Chapter 3 of this monograph.

It is expedient to start forming a national resilience ensuring model by determining the scope of the relevant system. This raises a debate, about how a national resilience ensuring system should be organized: as an independent subsystem of public administration (detaching a function) or as an improvement according to the resilience principles of the existing systems and their interconnections (cross-cutting approach). As shown above, the best option is to form a comprehensive national security and resilience ensuring system in a way where both system mechanisms would combine and complement each other. This is the way to achieve a synergistic effect of the interaction between different systems while rationally using the resources of the state and society. Considering the national resilience ensuring system from the standpoint of a separate public administration subsystem, we should mainly focus on the organization of links between all actors and objects, which allows carrying out adaptive management and purposeful self-governance within the system, finding a balance between centralization and decentralization of the management function, help strengthen the resilience of key objects and actors and their subsystems, as well as the resilience of the system as a whole.

A systematic analysis of a specific national resilience ensuring model allows for determining how effectively and promptly the system responds to signals from the security environment in the form of dangerous trends, processes, phenomena, and, ultimately, threats and crises. Analysis findings show compliance or non-compliance of the selected model with its operational objectives.

Different models of national resilience ensuring systems focus on achieving the common aim – to reduce dangerous impacts of threats and maintain continuous functioning of the essential life spheres of the society and state before, during, and after a crisis, including through adaptation to threats and rapid changes of the security environment. At the same time, priorities and direction of measures taken in these systems to achieve this aim also differ. This follows from peculiarities of selecting key operating parameters of the national resilience ensuring system, which implies that key actors compromise on core values, assessments of the security situation, methods and practical results of relevant activities, and selecting possible options to achieve the determined goals.

The expert community mostly often disagrees about what types of processes the national resilience ensuring model should be focused on. After having analyzed academic literature (Francart, 2010; Fjäder, 2014; Lentzos & Rose, 2009), it is expedient to highlight the following significant alternatives in research approaches to determining the main national resilience ensuring benchmarks:

- reducing the adverse effects of threats or ensuring a rapid post-crisis recovery;
- priority of preventive *or* reactive threat response measures;
- priority of measures on ensuring threat preparedness and forecasting *or* effective crisis management and building security capabilities.

Given the limited resource capabilities of the state and society, it is impossible to achieve all these goals together. Inevitability, unpredictability, or hard predictability of most modern threats are often the main argument in scientific and political debates. This explains why the national resilience ensuring model is mainly chosen in favor of reactive rather than preventive measures, in favor of rapid crisis recovery-enabling mechanisms rather than those mitigating threat impacts and ensuring continuity of socially essential functions at an acceptable level. In particular, this is highlighted by Francart (2010) who characterizes differences between the British and French models of national resilience ensuring system.

Fjäder (2014) argues that in order to implement the national security resilience concept, we need to find a new balance between preventive measures within the traditional national security model and reactive measures in the national resilience format. The scholar emphasizes that in contrast to conceptual approaches to national security, national resilience implies that key measures should aim to reduce not the likelihood of a threat but its impact on the state and society, and, therefore, not to prevent threats but to minimize disruption of essential services.

Researching the national resilience phenomenon, Lentzos and Rose (2009) concluded that the resilience logic is not just an attitude to preparedness; being resilient is not just about being protected or having emergency recovery systems. According to the scientists, resilience means systematic, large-scale, organizational, structural, and personal capability-building to anticipate and counter possible disruptions in difficult conditions, avoid collapse, overcome the crisis, and recover properly.

In practical terms, we can observe that states implement different broad or narrow approaches to the organization of the national resilience ensuring system within the selected model (Reznikova, 2020d). Within the *broad approach*, the resilience principles are implemented in all spheres of national security and public administration, including economic, social, environmental, foreign policy, etc., as well as in social relations. In particular, this approach has already been implemented in the Netherlands, Estonia, Finland, and New Zealand.

The *narrow approach* to national resilience implies basing primarily on improving crisis management in the field of protection of the population and state critical facilities from various threats and hazards (especially natural, man-made, biological, terrorist, or military), as well as providing business continuity of state critical functions (including governance, energy, water, and food supply, transport and communications, primary health care, the ability to cope with mass displacements, significant human losses or spreads of dangerous diseases, etc.). Here, the key universal resilience ensuring mechanisms are mostly the system of protection of the population from emergencies and the system of critical infrastructure facilities protection. The resilience principles have been most fully implemented in crisis management systems, in particular, in countries such as Norway, Denmark, Sweden, Great Britain, and the US.

In this context, Francart (2010) emphasizes that ensuring resilience is not identical to crisis management, which is a traditional element of governance. Rather, crisis management should be considered as one of the mechanisms allowing public institutions and society to counter threats. Besides, some authors' generalizations that "the national resilience concept came to the security theory from crisis management as a tool to recover from emergencies and natural disasters"[1] are simplistic and unfounded, because it is not the peculiarities of providing national resilience in a given country that determine the essence of the national resilience concept. On the contrary, the regularities of the relevant concept should be the basis on which states form their own national resilience ensuring models with due account for national interests and development features.

In practice, the narrow approach to ensuring national resilience is mostly used in states with developed democracies and economies, high well-being, and developed security capabilities that are members of powerful international alliances and organizations (e.g., EU and NATO). Experience has shown that the

[1] Melnyk, Yu. V., & Shypilova, L. (Eds.). (2019). Zabezpechennia natsionalnoi bezpeky Ukrainy v umovakh vkhodzhennia Ukrainy do Yevropeiskoho ta Yevroatlantychnoho prostoriv [Ensuring the National Security of Ukraine in Ukraine's Accession to the European and Euro-Atlantic Spaces]. Kyiv: National Academy for Public Administration. [in Ukrainian].

level of economic, social, socio-political, or foreign policy threats in such states is lower, although they also suffer from natural disasters or emergencies (floods, hurricanes, etc.). Given this, increasing civilian preparedness, response efficiency, and prompt recovery from emergencies or crises, as well as providing the continuity of essential processes in the state are more topical for developed democracies than ensuring consolidation of the society or state economic and social resilience.

The experience of counteracting the COVID-19 spread shows that it is important to develop crisis management, but this is not the only way to strengthen national resilience. Restrictive anti-epidemic measures introduced in many countries created additional risks and threats to national security in other areas: economic, social, information, etc., intensified public debate about possible reduction of the rights and freedoms of people, etc. This highlights the issue of determining effective mechanisms for comprehensive response to a wide range of threats at all stages, increasing the readiness of the state and society through the introduction of universal protocols of concerted action, as well as proper coordination of such activities and determining its clear legal limits (Reznikova, 2020b).

In general, the analysis of scientific literature and world experience gives grounds to argue that in order for the national resilience ensuring system to achieve its aims, the state should foster a range of processes, especially the following key ones:

- *assessing risks and their impacts, identifying threats, assessing capabilities, and identifying vulnerabilities* as a basis for strategic analysis and planning;
- *strategic analysis and planning,* aimed to balance many competing interests, including short-term and long-term, internal and external, public and private, financial and non-financial, as well as establishing state policy priorities

in ensuring national resilience and capability building; formulating action plans based on adaptive management, etc.;

- *providing readiness*, which implies disseminating necessary knowledge and skills, establishing partnerships between all national resilience actors, and forming a security and leadership culture;
- *crisis management*, which should ensure controllability and coordination of preparedness processes, effective response to threats and post-crisis recovery, accountability, information sharing, economic efficiency of measures, etc.;
- *forming a unified legal framework* to determine basic principles of ensuring national resilience, the national coordinator, and the general scheme of allocation of responsibilities and powers of state bodies according to national resilience ensuring branches;
- *establishing organizational mechanisms to ensure resilience, including at the regional and local levels*, which implies, in particular, creating permanent formats (structures) of interaction between state and local authorities, public associations, private businesses, and international partners in providing national resilience, as well as expert networks, etc.

Therefore, the issue of how to organize resilience management processes within the selected national resilience ensuring model is one of the most difficult and deserves scrutiny.

2.2.2. Methodological Foundations of Creating Mechanisms to Adaptively Manage National Resilience

Adaptive management of national resilience generally aims to keep the main operational processes and indicators of the state and society dynamically balanced. This can be illustrated by a homeostatic plateau graph developed by Van Gigch (1981b), improved by Kharazishvili (2019), and adapted by the author of this monograph (*Fig. 2.2*). The national resilience level as a generalized indicator, as well as the resilience levels of the state and society (including their individual subsystems and elements) to various threats, should not exceed critical values. If the general resilience level approaches the upper critical level R^{u}_{cr}, this indicates a high probability of falling into the rigidity trap, and if it approaches the lower critical level R^{l}_{cr}, it means a high probability of falling into the poverty trap. It is possible for certain indicators of specified resilience to temporarily exceed the critical values, which will not lead to the destruction of the state and society if they return to safe operation fast enough.

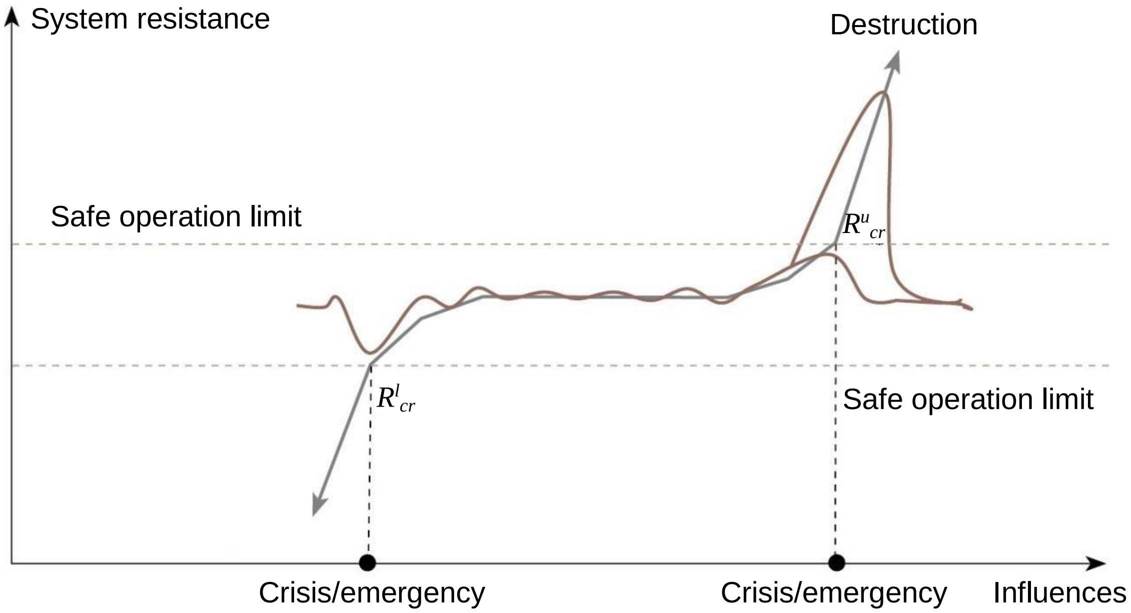


Fig. 2.2. Managing national resilience on the basis of the homeostatic plateau
Source: Van Gigch (1981b), Kharazishvili (2019) (adjusted by developed by the author).

As noted in Chapter 1 of this monograph, it is important to choose the optimal level of national resilience in general and the optimal resilience levels of its individual components (specified resilience levels) in order to form public policy in this field, as it sets clear guidelines. We should keep in mind that benchmarks determined without due account for the situation context and time frame can significantly distort state policy and disorient national security and resilience providers. Therefore, the optimal national resilience level and other benchmarks are variables that should be periodically reviewed and adjusted on the basis of adaptive management.

Providing national resilience brings together different branches and systems (including economic, environmental, social, organizational, military, law enforcement, etc.): all of them should meet basic resilience criteria. At the same time, the specifics of different branches should be taken into account while determining their benchmarks.

Among key national resilience management issues are resourcing and relevant capability building. Resources should be regarded as constraints in planning and implementing national resilience ensuring measures. Allocation of resources requires seeking compromises and balance of different interests not only within the state policy in national security and resilience but also between state policies of various directions.

World experience shows that many countries now apply a *comprehensive approach* to providing preparedness and effective response to a wide range of threats and rapid recovery after crises, according to which civil protection and crisis management issues are considered in combination with other aspects of national security and defense. This refers not only to the cooperation of authorized state bodies with the population and businesses within their area of responsibility but also to inter-branch and inter-sectoral cooperation. In other words, the whole-of-society and whole-of-government approaches are currently used to organize a national resilience ensuring system. In some countries, these approaches are implemented in the total or comprehensive defense model or comprehensive crisis management which form the basis of organizational systems used to manage national resilience. This allows solving the resourcing problem through joint capability building and achievement of resource efficiency by eliminating duplication of functions and clear allocation of powers in the national security and resilience ensuring system.

An important direction of adaptive management is *strategic analysis*, which allows increasing the readiness of the state and society to respond to threats and crises, as well as their adaptability to rapid changes in the security environment. Hence, strategic analysis has the following key directions:

- analyzing security environment;
- analyzing the state and dynamics of key parameters of the system in the context of changes in the security environment;
- analyzing lessons learned;
- studying long-term trends in the security environment.

Such an analysis allows us to timely identify threats and vulnerabilities of the state and society, adjust the relevant state policy, and, if necessary, the national resilience ensuring model.

It should be noted that analyzing the security environment and planning national security and resilience ensuring measures are often practically limited to state interests, while the needs of society are ignored. As the UK experience during the terrorist attacks on the London transport system in 2005 showed, the state's emergency plans were focused primarily on ensuring the safety of the transport system itself, rather than on ordinary citizens (Edwards, 2009). This leads to a conclusion that *national resilience should be managed comprehensively, and while strengthening the resilience of individual objects, not only their organizational and operational features but also the nature of interaction with other objects and actors should be considered*.

Changes in the security environment and key parameters of the national resilience ensuring system, identified by the strategic analysis, require in-depth research to lay grounds for effective state policy in this field. Gorbulin and Kachynskyi (2010) draw attention to the principles of social development which must be taken into account when developing a national security strategy. This means, in particular, the "non-zero (acceptable) risk principle", according to which it is necessary to try to achieve such a risk level in all spheres of life, which can be considered acceptable. This example supports the fact that *comprehensive risk and impact assessment, as well as identification of threats* *and vulnerabilities,* are important components of strategic planning and national resilience management.

Another important direction of national resilience management, that should be taken into account while developing the relevant adaptive management mechanisms, is to *ensure an appropriate level of readiness* to respond to threats of any origin and nature. All resilience ensuring actors should be aware of trends and processes taking place in the field of security, as well as the procedure and rules of interaction before, during, and after a crisis. To achieve this, proper legal support in the relevant field, effective crisis planning, development of education, in particular disseminating necessary knowledge on risks and threats, building crisis interaction skills, security culture, etc. are required.

The state and society increase their adaptability if, working together, they are able to elaborate and make non-standard innovative decisions, and transform negative results into positive ones, if possible. This may require *creating new organizational systems or reforming social relations in order to strengthen and develop system links*. The establishment of *critical infrastructure protection systems* can serve as an example of such kind of adaptive resilience management mechanisms effectively used in various countries. Such universal mechanisms allow increasing security and resilience level of facilities fundamentally important to provide continuity of essential life functions of the state and society and settle the interaction of various governmental and non-governmental structures (including private businesses) in a single organizational and legal mechanism.

For states with underdeveloped local self-government traditions, it is expedient *to carry out a power decentralization reform* that should involve the security sphere. In general, such an approach is in line with adaptive management logic and makes the national security ensuring system more flexible and able to provide a rapid threat response at the territorial level. At the same time, decentralization in national security is one of the most controversial issues, as in the framework of the world's most widespread liberal-democratic political system, the state is the main security contributor, and the military and law enforcement governance systems have a rigid state-centric hierarchy.

As noted above, within the practical implementation of the national resilience concept, it may be expedient to redistribute security powers between central and local authorities, while maintaining the key role of the state in addressing strategic national security and resilience issues and strengthening its control and coordination functions. Excessive concentration of power in one center increases the risk of disruptions in providing society with essential life functions if governance collapses. In view of this, a reasonable part of responsibilities and resources should be transferred to the local level. This also envisages creating or strengthening local security and defense capabilities, including units of territorial defense, civil defense, and public order, involvement of citizens' associations in active cooperation, development of state-private partnership in national security, etc. Decentralization in national security allows to counter a wide range of threats, including hybrid ones, and absorb them already at the local level more effectively.

Experience of countries with developed local self-government traditions (in particular, the United States and Great Britain) shows that strengthening the security component of local authorities is a possible and quite effective way to provide national resilience. We are talking, in particular, about establishing municipal police, units of local defense, reservists, etc. A characteristic feature here is introduction of the principle "anything that is not explicitly prohibited is permitted" instead of "exercise authority within the limits and in the manner prescribed by law" as the main principle of their activities. This significantly increases the flexibility of the national resilience ensuring system, which is especially important under uncertainty and changing security environment. At the same time, such a change in the principles of the security and defense sector activities requires forming an appropriate security culture and inevitability of liability for law violations, as well as improving the efficiency of civil control.

According to Fluri and Badrak (2017), it is the bottom-up initiatives that should become effective in improving the protection of the population from armed attacks and man-made and natural disasters, and if every citizen realizes that he is responsible for providing safety of his village/settlement, city, region, and, hence, his country, this is the best tool to create a comprehensive national defense system.

Among the examples of successful local security and defense forces are the National Guard and the decentralized police service in the United States, local police support forces in England, and local fire brigades in most Western countries. Involving public associations in cooperation with authorized state institutions on certain issues of ensuring national resilience is also widespread. Public-private partnership in national security is also developed.

In general, the *security and defense sector should be currently reformed* with due account for resilience principles to demonstrate the ongoing process of development of the relevant public agencies and their management systems, as well as their adaptation to new security conditions. In particular, it implies improving interagency interaction and cooperation with businesses and the public, as well as forming new organizational mechanisms.

While forming national resilience adaptive management mechanisms, it is very important to create and implement an *early warning system* to detect and prevent threats in the early stages, especially in the context of spreading hybrid threats (Reznikova, 2019b). Such threats are usually hidden or implemented by manipulating democratic values and legal mechanisms. It is very difficult to identify them at the initial stage and anticipate their development because of their non-linear nature.

Modern early warning systems consist not only of technical means to inform the public about an emergency, including a warning by special signals (sirens). They function to early detect threats and create conditions to absorb (if possible) or prevent them and mitigate their adverse impact on the state and society. The need to early detect and assess a wide range of threats, including hybrid ones, increases requirements for intelligence, counterintelligence, law enforcement, and other public agencies, because timely detection of threats in a particular area of responsibility is within their purview. Their organizational, analytical, technical, operational, and other capabilities are used for threat detection. In turn, this raises an issue of regular assessing security and defense sector capabilities to counter traditional and new threats. A comprehensive security and defense sector review, as well as a review of the resilience of public and local authorities, can be an effective tool to identify relevant vulnerabilities ("weak links" in the security and defense sector).

Situation centers that can be established at public authorities are an efficient tool to identify threats at an early stage and determine rapid response measures. Combining their efforts by creating a situational centers network allows the implementation of broad cooperation and a comprehensive approach to threat analysis. Chernyatevych (2012) concludes that situation centers are designed to address the following main tasks: to anticipate crises, to prepare managerial decisions to prevent (overcome) them, to anticipate situation evolvement, to monitor the situation according to the determined criteria, to elaborate possible scenarios and appropriate response measures, to assess possibilities of implementing managerial decisions, etc. In order to implement these tasks, a situation center should ensure that the following key functions are performed: collecting information about a particular area of activity; determining criteria for its assessment; data processing to identify influencing factors; constructing analysis models; elaborating managerial decisions and their implementation; monitoring and assessing outcomes of the implementation of the decisions (Chernyatevych, 2012).

In the context of providing national resilience, it is important to form a network of situation centers, but this is not the only element in the early warning system. The broad interaction (inclusion) principle implies that civil society should be actively involved at all stages of the national resilience ensuring cycle, and permanent bi-directional communication channels should be created. In this context, the experience of various countries is noteworthy: Great Britain – concerning operations of local resilience forums and the formation of the National Risk Register; the United States and Israel – concerning the involvement of the population in support of law enforcement agencies in combating terrorist activities and building public resilience to this threat; Estonia – concerning the role of civil society in identifying and countering threats in information sphere and cyberspace, etc. The OSCE Office for Democratic Institutions and Human Rights together with the OSCE Secretariat Department for Combating Transnational Threats has prepared a guiding report "Preventing Terrorism and Countering Violent Extremism and Radicalization that Lead to Terrorism: A Community-Policing Approach", which, in particular, describes how to involve specific categories of the population (youth, women, members of religious organizations, ethnic minorities, and representatives of small and medium businesses) (OSCE, 2014).

Efficient interaction between public agencies and civil society in the field of national resilience, including at the stage of early prevention of threats to national security, requires proper organization and coordination. In world practice, this function is mainly performed by an executive body or its specially formed service. For example, it is the Cabinet Office in the UK and the Federal Emergency Management Agency [FEMA] within the Department of Homeland Security [DHS] in the USA.

In order to create and implement national resilience adaptive management mechanisms, all actors should equally understand the nature of a threat, its manifestations, assessments, and the level, which requires an immediate response. Different perceptions of these matters by various public authorities and society may hinder coordinated efforts to prevent and combat threats, as well as the timely application of other national resilience ensuring mechanisms. World experience shows that the efficiency of a state's response to modern threats (especially hybrid) largely depends on how well actions of authorized state bodies are coordinated and to what extent other actors (society, individuals, businesses, and organizations) are involved.

The following measures usually contribute to fostering comprehensive whole-of-society cooperation in national resilience: introducing common terminology and methodological principles in threat identification and risk assessment; producing and distributing relevant information and demonstration materials for the population; and conducting outreach and educational activities. Scientific institutions, educational establishments, and think tanks should be engaged in such activities.

At the stage of early detection and prevention of threats, the most difficult is to identify and assess hybrid threats as they are hidden, can become apparent over time, and have no clear criteria to be identified and assessed. Highly-trained professionals with relevant work experience should be involved in these activities. Considering how situation centers are organized, Chernyatevych (2012) notes that the more precisely the analyst intuitively captures real, objective processes, the more efficient will be his conclusions and recommendations obtained through formal (mathematical) methods.

For early threat detection and identification, it is necessary, first of all, to determine the main spheres where the situation will be constantly monitored. In particular, to this end, we can focus on traditional national security spheres: military, economic, social, foreign policy, information, cybersecurity, environmental, etc. Such operational work should, of course, go along with strategic analysis, which will allow quickly adjusting state decisions and security activities with due account for the identified trends and potential threats.

To ensure the effective operation of the early warning system as part of the network of situation centers, it is expedient to develop *threat data sheets (threat passport)*, which should define characteristic events, phenomena, and processes that enable to identify threats (early signals), threatened objects, factors influencing the emergence and development of a crisis, the source of danger, possible impacts to national security, etc. (Reznikova, 2018e). Determining early warning signals about threats is a rather complex, even creative process, during which both traditional and informal methods of analysis, such as intuitive-logical, formal-logical, operational-applied, analytical-prognostic, etc. should be used. In particular, early manifestations of terrorist and military threats, economic crises, and natural disasters have been sufficiently explored in world practice. Identification and early prevention of hostile external influences (political, ideological, cultural, financial, etc.), risks of conflict in society, information attacks, etc. require further research.

Given that current threats are complex and dynamic, information processing means and methods of the early warning system should be periodically updated. Due to the above, we can argue that it is very important for national resilience adaptive management to provide the development of technical capabilities of the situation center network, periodically train expert analysts, and foster inclusive interaction.

In addition to introducing universal national resilience adaptive management mechanisms, it is also expedient to strengthen resilience to certain threats (terrorist threats, information influences, emergencies, etc.) in certain national security areas through the development and implementation of special mechanisms and practices. This requires taking into account the operational features of the relevant branch and the nature of its inherent threats.

States usually begin to apply resilience mechanisms in their priority areas, the most typical of which currently are counter-terrorism, critical infrastructure protection, cybersecurity, response to man-made emergencies and natural disasters, business continuity, etc. The implementation of such mechanisms starts with the development and adoption of appropriate programs, action plans, guidelines, recommendations, etc.

In general, an efficient organization of national resilience adaptive management processes depends not only on the understanding of its aim and the mechanisms but also on its ability to ensure *governance continuity*. To achieve this, it is necessary to implement a set of precautionary measures, in particular:

- to develop basic and create reserve capabilities, as well as alternative development plans and strategies to ensure the state can perform its minimum necessary socially important functions during a crisis and promptly recover in the post-crisis period;
- to develop and implement schemes for allocation of responsibilities and replacement of key governance positions;
- to form communication channels that allow to make, explain and implement government decisions in compliance with the principles of legality, efficiency, and accountability even in crises.

We should also emphasize that it is important to timely implement a set of measures to ensure cybersecurity and information protection in authorized state bodies, including in the situation centers network, as well as to form a high-quality staff pool in the field of national security and resilience.

2.2.3. Defining National Resilience Providing Priorities

It is impossible to provide a high level of preparedness to respond to all threats and crises that may arise in today’s world. As noted in Chapter 1 of this monograph, not all objects may be equally resilient, and the resilience level may vary in different areas depending on the situational context and other factors. The need to maintain the basic system parameters within the safe function limits under a significant number of threats that states and society are facing today and limited resources to counter threats require *determining* national resilience providing *priorities*. This complex issue is solved through a compromise and balance of interests of all national resilience actors with due account for national interests, assigned objectives, and guidelines in the relevant field. In particular, Anderies and Martin-Breen (2011), and Chandler (2014) studied how to prioritize measures and resolve possible conflicts of interest in ensuring national resilience.

A number of objective and subjective reasons determine which priorities will be chosen due to different understandings of the national resilience concept and different assessments of major threats to national security by politicians and experts involved in the relevant public policy development, as well as external obligations of the state, including related to its membership in certain international organizations, etc. Possible divergence of views on national resilience can be illustrated by a study conducted by a group of researchers from Israel and Canada who interviewed students of a number of Israeli and US universities to determine how respondents understand the “national resilience” term and key threats to the state (Canetti et al., 2013).

These two questions were selected for the survey quite reasonably, as the national resilience and the national security systems are closely interconnected, and if resilience mechanisms to the determined threats are introduced, the effectiveness of countering these threats rises at all stages of the crisis cycle (including prevention or minimizing possible adverse impacts, response, and recovery to full functioning). Countries were also selected purposefully, as they have many common features. In particular, both are democracies with a population formed mainly of immigrants, with developed economies and high social standards. Besides, both countries have long suffered from terrorist threats.

Despite these common features of the selected states and their societies, the results of the survey revealed some differences both in respondents’ assessments of key threats and their understanding of national resilience, as noted in Chapter 1 of this monograph. Although terrorism ranked first in national security threats in the total number of responses, the level of concern about this threat among Americans was almost twice as high as among Israelis. The researchers explain this by the higher levels of readiness of the Israeli security and defense forces and population to counter terrorism, public confidence in the national security and defense forces, as well as constantly strained relations with some neighboring states. Israelis have been facing the situation for a long time, so they have adapted to it and learned to maintain a fairly high standard of living and security in the country. At the same time, the USA had a very negative experience with the devastating terrorist attacks of September 11, 2001 (Canetti et al., 2013).

According to the aforementioned survey results, there were other differences in perception of key threats to these countries. For Israelis, most threats were related to military, geopolitical, and socio-economic spheres. The surveyed Israelis were considerably concerned with significant social gaps between different groups of the population and internal political differences in the country. On the other hand, Americans were more concerned about threats from inefficient governance, deterioration of the environment and public health, and increasing traffic accidents rate. From a geographical perspective, the Americans identify the main threats as coming from China and Iraq, while the Israelis identify them as coming from Iran, Palestine, and a range of Arab states. Respondents from both countries showed the smallest differences in their assessments of such threats as economic instability (ranked second after terrorism), war, poor education, and political mistakes (Canetti et al., 2013).

Therefore, even under similar basic conditions, different people’s perception of threats is influenced by certain national peculiarities: geographical, cultural, historical, socio-economic, etc. In general, threats faced by different countries may differ in nature and origin. Although the national security systems of different states are generally similar and focused on counteracting a wide range of threats, each state may have different priorities in implementing certain national resilience ensuring mechanisms and peculiarities of forming an appropriate model, which depends, inter alia, on identifying key national security threats (Reznikova, 2019c).

As national resilience mechanisms require some time and resources for their implementation, they are difficult and sometimes impractical to implement simultaneously. Based on the results of the above-mentioned observations, we can draw the following conclusions, which, if practically implemented, will allow determining priorities in ensuring national resilience more objectively and reasonably:

1) priority should be given to universal mechanisms and measures aimed at a comprehensive response to a wide range of threats and crises at all stages of the crisis cycle (which implies, in particular, creating new organizational systems, implementing comprehensive measures based on the society's participatory involvement (inclusion), etc.);

2) is more appropriate to introduce special resilience mechanisms for certain threats and crises (including from the perspective of key target groups) if these threats meet the following criteria:

- their likelihood is high (for example, the country is located in a seismically active zone);
- they may have a devastating and large-scale impact (for example, mass casualties, destruction of critical infrastructure, economic collapse, etc.);
- they cannot be prevented and completely overcome (for example, earthquakes, floods, terrorism, etc.);
- they have dynamic, long-lasting, and complex nature (for example, hybrid threats).

Many countries face the challenge of selecting priorities in providing national resilience and effectively combining appropriate mechanisms with traditional national security measures. In particular, Japan has developed appropriate recommendations based on studying the experience of the largest disasters in its history (National Resilience Promotion Office of the Cabinet Secretariat of Japan, n.d.).

Taking the conceptual bases of ensuring national resilience into account, we can argue that the need to mitigate the adverse influence of threats and adapt to high levels of uncertainty in the security environment requires establishing certain benchmarks. National resilience ensuring mechanisms and measures should be aimed to achieve them. To develop such benchmarks, it is necessary to identify, in particular:

- impacts of the threat that must be mitigated or minimized;
- objects (facilities or people) that may be most affected by the threat;
- the main ways to minimize and overcome the impact and the relevant capabilities required;
- processes and/or values in/of the state and society that must remain unchanged under threat (for example, lifestyle, guaranteed rights and freedoms of citizens, environment, governance and business continuity, etc.)

Experts usually argue about the latter point most of all. For example, American society has agreed on the need to restrict certain rights and freedoms of citizens in favor of strengthening the state counter-terrorism system. Meanwhile, in the UK, the national resilience ensuring mechanisms are designed in such a way that they do not reduce the rights and freedoms of citizens in any way and do not change the British lifestyle, according to Francart (2010).

A comprehensive review of the national security ensuring system allows identifying vulnerabilities that hinder the effective countering of identified threats at various stages within the traditional security paradigm. Timely detection and elimination of these and other vulnerabilities of the state and society requires the development and implementation of such national resilience ensuring mechanisms, which will operate on a permanent basis and adapt to today’s complex security environment. According to the regularities revealed above, such mechanisms may be formed in two main directions, namely:

- strengthening capabilities of the state, regions, and local communities in countering threats and crises;
- introducing new processes, forming new systems (organizational, technical, etc.) allowing to adapt to the continuous adverse influences.

In practice, any combination of these measures can be used. It would be appropriate to highlight a group of measures aimed to strengthen social resilience, such as forming a security culture, the necessary knowledge, and skills, etc. Here, as Japanese experts note, the most valuable are universal (systemic) national resilience ensuring mechanisms which include forming a national risk assessment system (National Resilience Promotion Office of the Cabinet Secretariat of Japan, n.d.).

2.3. Risk and Capability Assessment, Identification of Threats and Vulnerabilities in National Security

2.3.1. The Expediency of Establishing a National Risk Assessment System

As already mentioned, uncertainty and changeability are signs of the modern world. Fiksel (2006) argues that predictability has become an anachronism and decision making must occur in the context of a wide spectrum of changing possibilities. This calls into question the reliability of forecasts, especially long-term, developed in the security sphere and the possibility of using such information to form appropriate state policy.

Under such conditions, the assessment process as a national resilience management component requires certain adjustments. Anticipating the future (especially likely threats and crises) is less valuable than finding solutions that provide security policy flexibility and actors' readiness to respond to threats and crises. It has been proven that in the context of ensuring national resilience, it is more expedient to use the adaptive management model, which important part is assessment, according to Holling (1978). As the scientist argues, assessment should be continuous, as they provide information essential to selecting and adjusting ways to further develop and adjust the policy.

As noted in Chapter 1 of the monograph, the state and functionality of a system and its individual elements can be assessed for their compliance with the resilience criteria. At the same time, it is equally important to *assess risks* in the context of ensuring national security and resilience. We are talking about influences coming from the external and internal security environment. Risk assessment allows for timely detection of trends both dangerous and promising for the development of the state and society and identifies threats and vulnerabilities. This ultimately helps formulate strategic documents of the state and action plans in case of crisis, and allows their timely amending, etc. Given that risks to the state and society may arise in different areas and have different consequences, they should be analyzed comprehensively and systematically.

It should be noted that the terms “risk”, “threat”, “challenge”, “hazard”, and “vulnerability” have different definitions in the scientific and professional literature, and there are different research approaches to determining the links between them. These words are often used interchangeably. In particular, Brauch (2005, 2011) deals with these problems. The scholar addresses not only the lexical meaning of these terms but also their concepts and historical transformations. However, even this scholar does not give an unequivocal answer about how these terms relate. In view of this, the terms will be used in the monograph according to the following definitions from international standards:

risk – an effect of uncertainty on objectives (ISO, 2018a);

threat – a potential cause of an unwanted incident, which could result in harm to individuals, assets, a system or organization, the environment or the community (ISO, 2021).

It should be emphasized that risk is only probable but not a guaranteed unwanted result caused by certain events, activities, etc. At the same time, threats are directly related to certain events, actions, or inactions of people, organizations, and states that may or intend to cause harm/losses to others. Currently, there are methods to assess both risks and threats.

Researchers identified the effective functioning of the risk assessment system as an important element in early threats detection and prevention, strategic planning, and providing national security and resilience. Such systems are called national because they operate at the state level, cover processes related to ensuring security of the state, society, and every citizen, and are based on broad interagency liaisons and cooperation (Reznikova, Voytovskyi & Lepikhov, 2020).

Applying modern risk assessment and threat identification methods and technologies, crisis modeling, and development of probable scenarios – all these allow increasing the reliability of the results, as well as forming a broad evidence base for further analysis. In conditions of rapid and unpredictable changes in the security environment, the general review of threats is much less valuable than typologies, multicriteria matrices, model catalogs, and probable scenarios developed on its basis. It is these that are needed to further determine concerted action protocols to respond to threats of various kinds and origins, as well as to plan appropriate measures.

National risk assessment systems operate in many countries around the world. As the world experience shows, despite some differences in the organization of such systems, all of them have a number of common characteristics, such as their purpose and the main directions of use of the obtained results (*Table 2.1*).

Table 2.1

Common Features of National Risk Assessment Systems

Characteristic	Manifestations
System purpose	• Assessing and ranking all possible risks for the state and society; • identifying dangerous trends and threats to national security; • searching for new state and social development opportunities; • identifying vulnerabilities in the state and society; • forming databases regarding risks, threats, and their impacts; • sharing information on national security risks among experts.
Directions where assessment results are used	• Adjustment of state policy in national security and resilience; • drafting state strategic and program documents; • developing national security and resilience mechanisms and individual measures; • forming plans and protocols of concerted actions regarding response to threats or crises of any origin at their different progress stages; • informing the public about current and future threats and crises

Source: developed by the author.

The main aim of the national risk assessment system is to determine typical groups of risks and their impacts on the target groups, assess risk likelihood, and the possible scale and severity of their impacts. After the relevant information is analyzed, universal protocols of concerted actions to respond to major threats and crises at their different progress stages should be developed.

Specific methods can be used to assess risks in various areas. However, it is extremely important to develop and implement a common methodology to assess risks and their impacts and identify threats to national security, as it will allow cross-cutting comparing and ranking of risks in different areas based on common principles and criteria. Besides, applying a unified scale for all types of risks will help increase the objectivity in setting priorities of ensuring national security and resilience.

Also, national risk assessment systems allow identifying dangerous trends and threats to national security and vulnerabilities in the state and society. The obtained information is used by the state leadership and authorized state bodies to make decisions on forming and implementing the relevant state policy, planning measures to increase the readiness of the state and society for a wide range of threats, building necessary capabilities, and allocating state financial resources. The national risk assessment system is an element of national security strategic planning in developed countries. A general scheme of the national risk assessment system functioning, which consists of collecting and analyzing input data and obtaining intermediate and final data processing results, is shown in *Fig. 2.3*.

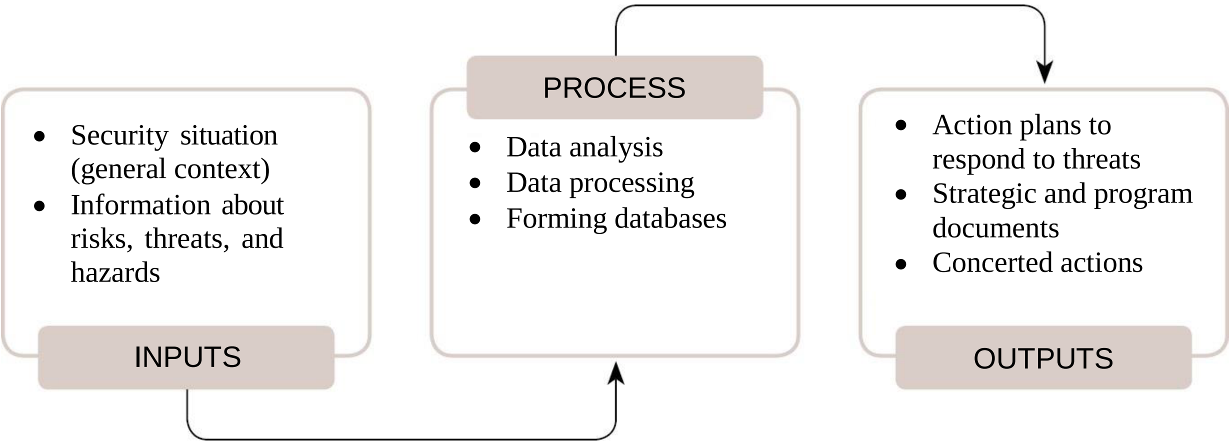

• Security situation (general context)
• Information about risks, threats, and hazards
INPUTS
PROCESS
• Data analysis
• Data processing
• Forming databases
• Action plans to respond to threats
• Strategic and program documents
• Concerted actions
OUTPUTS

Fig. 2.3. A general scheme of the national risk assessment system operation
Source: developed by the author.

According to a study of operation peculiarities of national risk assessment systems in various countries, we can conclude that such systems usually aim not only to identify risks and threats to the state and society but also cover more processes related to providing national security and resilience and comprise an algorithm for comprehensive risk and capability assessment and threat and vulnerability identification.

2.3.2. Algorithm for Comprehensive Risk and Capability Assessment and Threat and Vulnerability Identification

Different countries may use different risk assessment methodologies. According to recommendations of leading international organizations (OECD, 2017; United Nations Conference on Trade and Development [UNCTAD], 2020; United Nations Development Program [UNDP], n.d.) and the analysis of the best world practices in this field, presented in Chapter 3 of the monograph, we can distinguish *key stages* of comprehensive risk assessment (Reznikova et al., 2020).

Stage 1. **Security situation analysis**

At this stage:

– the general situation context is identified;

– key national security indicators in various areas are compared with their determined critical values;

– dangerous trends and new opportunities for the development of the state and society, including long-term, are identified.

Stage 2. **Identification of the greatest risks to national security, identification of threats (screening)**

Two main methodological approaches are used to achieve this aim:

1) assessment of all available risks according to the criteria of likelihood and severity of impact. The Delphi method is usually used for such analysis. As with any expert survey, the disadvantages of this method are certain subjectivity of assessments, different professional levels of experts, possible manipulations of those who summarize the results, etc.;

2) at the beginning, the security environment is analyzed in terms of certain areas (e.g., economic, social, socio-political, environmental, etc.) in the dynamics according to the determined indicators. Countries often focus on national security areas where continuous monitoring and risk analysis are mandatory. Analyzing the security environment in these mandatory-inspected

areas allows to identify dangerous trends and indicators approaching to critical limits, as well as to narrow the list of risks for further analysis in terms of likelihood and severity of impacts. Here, subjectivity may be lower, as statistical indicators are also used in addition to expert assessments in such analysis.

Various logarithmic scales and special research methods are used to assess and compare risks. This allows identifying a number of risks that require the most attention and have the highest likelihood and the heaviest impacts. Besides, to make further analysis and develop anticipated scenarios, this list may be supplemented by risks with the greatest negative impact but low likelihood, as well as highly likely risks with insignificant impacts.

Smil (2012) classifies global risks according to their likelihood. Accordingly, the scholar identifies the following main risk groups: a) known disasters, which likelihood can be assessed because of their periodic nature; b) possible catastrophes that have never happened before; c) theoretical catastrophes, which likelihood can be estimated only theoretically. Smil (2012) uses mortality rates (in particular, the number of fatalities during 1 hour of impact per 1000 population) in order to assess the highest possible impact of a global catastrophe if the relevant risk comes true. Estimates of this scientist are based on the likelihood of a phenomenon or process in the next 50 or 100 years, as well as the scale of its likely impact.

The methodology used by the World Economic Forum experts to assess global risks is based on various research methods, including questionnaires, analysis, generalization, extrapolation, systematization, classification, and ranking (WEF, 2013). The conducted survey used the conclusions of experts, who, in turn, used other research methods, which increases the objectivity of the results, according to WEF (2013). At the same time, this methodology cannot be called very accurate if we compare the anticipated risks with actual events from previous years. Besides, this methodology does not identify links and influences between various global risks, and the possibility of emerging risks and cascading effects cannot be currently assessed or forecasted. Nevertheless, the World Economic Forum researches allow identifying current and projected global development trends.

In general, the shortcoming of both of the above methodological approaches to identifying the greatest risks and threats to national security is that they are based mainly on retrospective analysis. Hence, the sample of risks and threats includes mainly those of them that have already been identified or are well known. Meanwhile, the risks and threats comprising a group of so-called “black swans” (unpredictable or hard-to-predict events) are not taken into account. To address this issue, the risk assessment process should involve experts and organizations that conduct alternative security environment studies. It also allows the prevention of groupthink.

Other problems of risk assessment include a lack of analysis of risk reciprocal influence, especially if risks are from different areas, as well as incompatibility of assessments obtained by different methods (e.g., quantitative and qualitative).

In addition to assessing risk likelihood and impacts, it is also important to have the following information for further threat identification and ranking:

- acceptable risk level under the determined conditions;
- how a threat impacts a main branch or activity in focus, target groups, and other branches;
- additional factors that negatively influence the national security and increase the impact of the identified threat.

***Stage 3.* In-depth analysis of possible consequences, development of anticipated scenarios, and crisis modeling**

Every risk has certain consequences, including:

- dangerous impacts on the livelihoods of people, society, and the state, which can be both typical for a certain group of risks and atypical;

- creating new opportunities that may provide some impetus for development.

A set of risks and their consequences comprises a multidimensional matrix that is used for further analysis.

The total rate of possible consequences of each risk should be estimated according to criteria of severity, quantity, duration, etc. An in-depth analysis of such consequences may change the priority of the major identified threats.

Taking the world experience into account, in order to assess risk and threat impacts, it is recommended to determine their influence on the following *key object groups*:

- physical objects (residential and office buildings, networks, etc.);
- human capital (life, health, and public welfare);
- economic and financial resources;
- environment (natural resources, environmental situation, etc.);
- social and political capital (formal and informal social relations and networks, governance systems, political institutions, peace and security, etc.).

According to the needs of a branch or social relations sphere, *special target groups* can be singled out (i.e., children, people of working age, retirees, etc.).

It is recommended to identify target groups that may be most adversely affected by an impact, as well as those with sufficient resilience potential, able to independently counter the threat with the acceptable loss of functionality. The level of acceptable losses should be determined individually for each target group with due account for its key characteristics and features.

Also, in order to further develop anticipated scenarios and crisis models, it is necessary to determine the limit of acceptable risk for the state and society under the determined conditions. We are talking about a group of indicators characterizing possible risk impact on key areas – allowable losses that will not have a devastating impact on the condition and functionality of the state and society.

It is expedient to establish key protection objectives for different target groups to determine such indicators. In particular, *for the population*, such objectives may be to preserve life, health, personal property, etc. The following indicators should be used to assess the consequences of threats for these protection objectives: the number of casualties, fatalities, refugees, and internally displaced persons due to an emergency or crisis; the level, scale, and speed of spread of dangerous diseases; material and financial losses, etc. *For a state*, key protection objectives may be performing socially important functions: ensuring territorial integrity and state sovereignty, economic stability and sustainable development, public safety, governance continuity, supply of drinking water, food, energy resources, etc. In order to assess threat consequences for the relevant protection objectives, the following indicators should be used: the possibility of territorial loss, the emergence of destructive processes in society, destruction of critical infrastructure facilities, economic losses, etc.

Criteria to analyze risk and threat consequences may vary from country to country. In the USA, the main objects of possible risk and threat impacts are recognized as both the state and the population in general and critical areas, including social relations, economy, environment, and public administration.

To assess risks and identify threats in a particular brunch or industry (area of responsibility), it is recommended to use the following main groups of indicators:

- indicators of the security in the area;
- threat likelihood;
- the scale of likely impacts.

Anticipated scenarios are developed and crises are modeled with due account for the data obtained. An anticipated scenario can be ranked using comparative analysis methods and various criteria and assumptions. After ranking, priority scenarios are considered in three versions: optimistic, pessimistic, and realistic with due account for the determined acceptable risk limit. It should be added that it is difficult to avoid subjectivism at this stage of the analysis, as scenarios are anticipated by experts with different professionalism and life experience. Besides, there is a degree of uncertainty about the future in general. Therefore, the required correction factors can be applied when developing and comparing different anticipated scenarios.

To develop protocols of concerted actions at different stages of threat response, it is important to group typical consequences of risks and threats of various nature and origin, as well as types of typical factors influencing the development of various crises. Timely decision-making on taking risk mitigation measures shows that the state has efficient national security and resilience policy which should be developed with due account for acceptable risk limits and anticipated scenarios. Recommendations on risk assessment and management could be found in the relevant international ISO standards, in particular in ISO (2018a), and ISO (2019a). However, it should be noted that these recommendations are generic and do not preclude further development and adjustment of their provisions for different areas.

***Stage 4.* Capability assessment**

In some countries, risk assessment completes after the above-mentioned steps not taking into account capabilities needed to address current and future threats to national security. However, this capability assessment is essential in the context of further planning of measures needed to respond to threats and crises and increase response readiness of the state and society. It is expedient to assess security capabilities during or following a review of the security and defense sector and its individual components, in particular in the context of providing the continuity of essential state functions, proper organization of crisis management, etc.

A comprehensive national risk assessment system should include assessing the capabilities needed to effectively respond to threats at different stages of the crisis development cycle. Comparison of capabilities assessments with risk and threat assessments allows identifying vulnerabilities of the state, society, and national security and resilience ensuring system and taking timely measures to eliminate them.

So, when assessing capabilities, it is expedient to identify the ability of state institutions, systems, and organizations to effectively respond to crisis or threat development in terms of the following stages of the national resilience ensuring cycle:

1) *providing response preparedness*. At this stage of the national resilience ensuring cycle, it is recommended to use the following *key assessment criteria*:

- reliability (availability of necessary resources, regularity of legal and organizational aspects of activities, dissemination of necessary knowledge and skills among responders, training, taking threat prevention measures, etc.);
- redundancy (availability of reserves in terms of all types of resources with due account for branch-related peculiarities and contingency levels);
- adaptability (availability of alternative sources of ensuring critical state functions, development strategies, response plans to various anticipated scenarios, as well as flexibility and efficiency of management (including crisis management) systems);
- absorption (ability to deal with a significant number of casualties, internal displaced persons, and refugees, provide necessary social support, medical care, etc.)

From the perspective of *providing the state's critical functions continuity, it is recommended to assess*: the availability and reliability of alternative sources and chains to supply the population with drinking water, food, and electricity; availability and reliability of alternative sources and chains to supply electricity and drinking water to administrative buildings; availability and reliability of alternative premises where state institutions, strategic enterprises and their employees, internal displaced persons, medical institutions and casualties may be temporarily relocated; reliability of communication and cybersecurity systems; security of data storage and transmission systems, the possibility of remote operation, in particular, taking into account the need to protect restricted information; availability and reliability of alternative transport routes, etc.;

2) *response*. During this stage of the national resilience ensuring cycle, it is recommended to assess: the existence of protocols of concerted actions in a crisis, which determine primarily universal mechanisms for responding to typical groups of situations; the ability to quickly attract additional (reserve) resources; clarity of division of responsibility and procedure of coordinating branch activities; efficiency of interagency interaction, crisis management, etc.;

3) *recovery*. During this stage of the national resilience ensuring cycle, it is recommended to proactively elaborate forecasts and possible scenarios of crisis development and recovery, including according to time criteria; to determine the acceptable level of losses for key target groups (according to the determined branch security and other indicators), etc. Taking necessary precautions should also be considered when developing and comparing anticipated scenarios, in particular as a correction factor.

Based on the basic national resilience criteria, public and local authorities, institutions, enterprises, and organizations can draw up lists of questions for *self-assessment on resilience*.

It should be noted that, according to the OECD (2017), currently available opportunities to assess risks and compare them with the state and society's capabilities to counter them are virtually unused by states to develop financial strategies for countering emergencies and crises.

***Step 5.* Identification of vulnerabilities**

Vulnerability can not only result from poor protection of an object from external destructive influences but also indicate that the object (system) has certain internal shortcomings or problems. Given this, vulnerabilities can be identified in several ways.

First of all, comparing risk and threat assessments with the level of the relevant capabilities allows identifying vulnerabilities of the state, society, and various branches/spheres of activity to certain types of threats. We are talking primarily about weaknesses in the national security and resilience ensuring system. They usually result from the lack or underdevelopment of the relevant capabilities, as well as the inefficiency of organizational liaisons between various national resilience providers. Early analysis of this issue allows elaborating an action plan to eliminate the identified vulnerabilities, develop capabilities and strengthen resilience.

Besides, if major objects, their subsystems, and elements have been assessed according to resilience criteria (including through self-assessment in government institutions, organizations, etc.), then it is possible to identify their inherent vulnerabilities. During such an analysis, it is expedient to take into account not only features of the objects but also certain characteristics of social relations: the level of public confidence in actions of the government and other state and local authorities; prevailing public moods; the efficiency of communication between the state and the population; maturity of security culture; the level of patriotic education, etc.

***Stage 6.* Comprehensive mapping, geospatial support**

Geospatial data analysis is a modern high-tech method to assess the security situation and identify threats. It allows combining existing state databases (meteorological, geological, infrastructural, medical, etc.) into a single real-time geographic information system which enables forecasting based on results of continuous monitoring. A general operating picture is established because information is gathered, sorted, generalized, and processed using analytical and technical means. Information on situation evolvement is provided to the concerned authorized structures. This information system can be filled with data, inter alia, through the situation centers network. The situation centers may have constant access to information processed by the system.

The advantage of this information system is that it allows analyzing many risks in space and time, taking into account their mutual influence, and comparing them with existing capabilities. This makes interagency cooperation more efficient, eliminates duplication of work, and creates conditions for decision-making based on real data.

For example, the geospatial data platforms created in the US cover basic data arrays, which include:

- static data related to human geography, critical infrastructure and key resources, asset inventory (equipment, supplies, personnel) etc.;
- data on specific events: situational data (route closures, damage assessments, etc.), derived and modeled hazards (flooded areas, the spread of dangerous diseases or substances, etc.), and field data (personnel, forces and means, etc.)[2].

At the same time, the geospatial system may have difficulties with integrating different databases and information systems, cybersecurity and information protection, data management, data storage, sharing access to the information system, its technical support, etc.

It should be noted that such high-tech information systems are not currently widespread in all countries.

***Stage 7*. Dissemination of risk assessment results, visualization**

Most often, a comprehensive report on the identified threats, anticipated scenarios of crisis, and their consequences (or a part of it) is considered confidential and not subject to disclosure.

[2] Lancaster T. *Geospatial support to resilience*. Report presented at Civil-Military Emergency Preparedness Program. Interagency Resilience Workshop #1, February 8, 2020, Kyiv, Ukraine.

Usually, the authorized organization also maintains a public *risk register*. It explains to citizens in a simple and clear way what dangers they may face in their daily lives, what their impacts are, how they may manifest, how to respond to them, and which authorities to contact. Such national risk and threat registers are publicly available, in particular on the official government websites of the United Kingdom[3], New Zealand[4], the Netherlands[5] and other countries. This allows increasing public awareness about the nature and manifestations of the main threats and hazards, as well as public readiness to respond.

***Step 8.* Monitoring and re-assessment of risks based on lessons learned**

According to the adaptive management principles, the results of risk and capability assessments and threat and vulnerability identification should be periodically reviewed and updated. In most cases, it should be done once in 1–5 years.

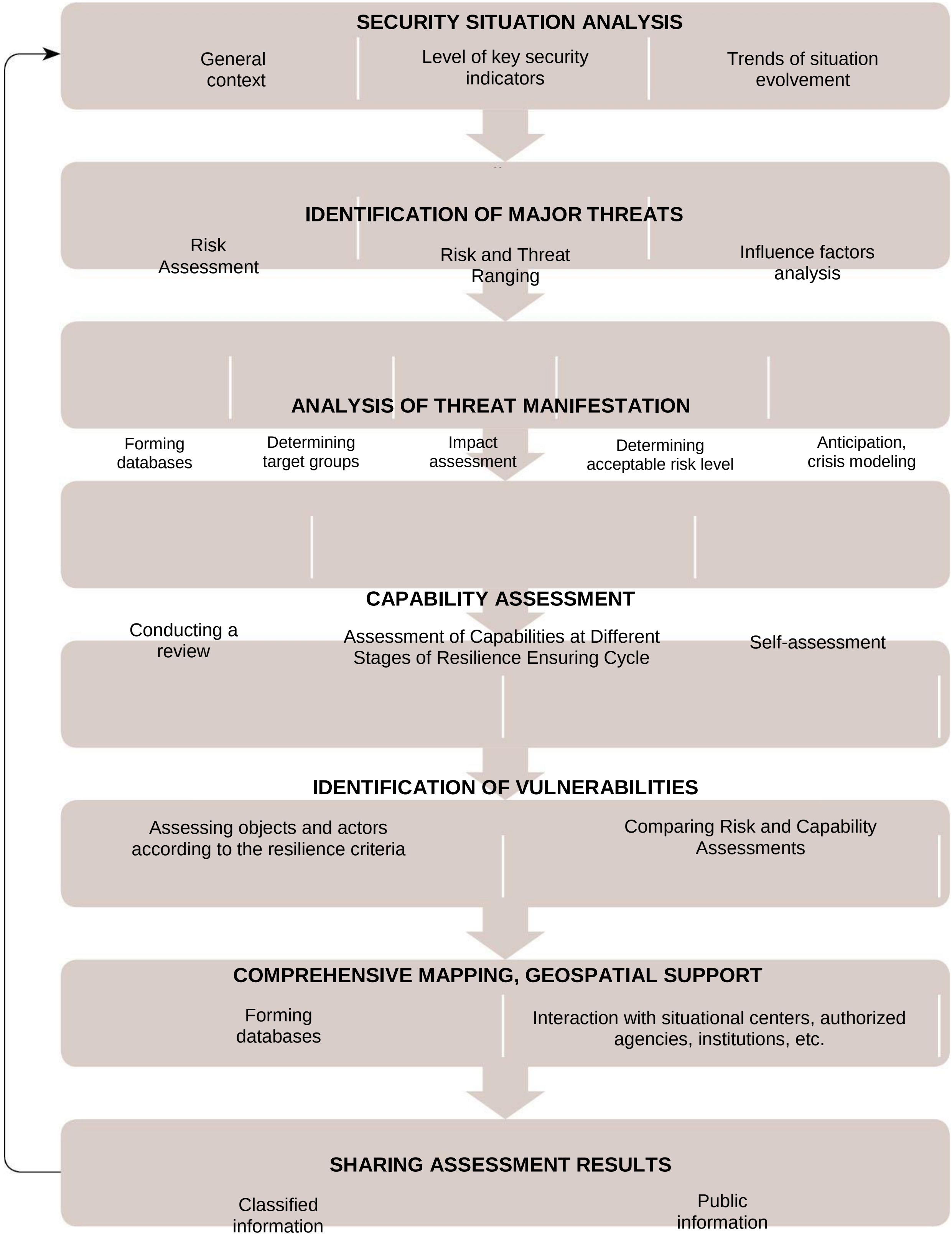
In generalized form, the algorithm of comprehensive risk and capability assessment and threat and vulnerability identification is schematically shown in *Fig. 2.4*. The proposed algorithm begins with the analysis of input data, which may differ for different branches/areas of activity during crisis development. For example, during the COVID-19 pandemic, the input data in the biosafety area concerned the spread of this dangerous disease, and in the economic area, input data concerned restrictive measures and their impact on businesses and society. At the same time, in the biosafety area, the typical measures comprising the basis of universal crisis concerted actions protocols are those used to prevent the spread of dangerous diseases regardless of their type, and in the economic area – those that should be used regardless of processes that have interrupted business (restrictive quarantine measures, natural disasters, hostilities, etc.) The basis of

[3] *See:* https://www.gov.uk/guidance/risk-assessment-how-the-risk-of-emergencies-in-the-uk-is-assessed#the-national-risk-register

[4] *See:* https://www.police.govt.nz/about-us/publication/national-risk-assessment-nra

[5] *See*: https://english.nctv.nl/documents/publications/2019/09/18/dutch-national-risk-assessment

strengthening national resilience consists precisely of actions aimed to develop and implement relevant measures to prevent threats, crises, and their consequences, form alternative strategies and action plans, and increase the preparedness of the state and society to respond to threats of any origin (outputs in the proposed algorithm).


SECURITY SITUATION ANALYSIS
General context
Level of key security indicators
Trends of situation evolvement
IDENTIFICATION OF MAJOR THREATS
Risk Assessment
Risk and Threat Ranging
Influence factors analysis
ANALYSIS OF THREAT MANIFESTATION
Forming databases
Determining target groups
Impact assessment
Determining acceptable risk level
Anticipation, crisis modeling
CAPABILITY ASSESSMENT
Conducting a review
Assessment of Capabilities at Different Stages of Resilience Ensuring Cycle
Self-assessment
IDENTIFICATION OF VULNERABILITIES
Assessing objects and actors according to the resilience criteria
Comparing Risk and Capability Assessments
COMPREHENSIVE MAPPING, GEOSPATIAL SUPPORT
Forming databases
Interaction with situational centers, authorized agencies, institutions, etc.
SHARING ASSESSMENT RESULTS
Classified information
Public information

SITUATION MONITORING, LESSONS LEARNED

Fig. 2.4. Algorithm for Comprehensive Risk and Capabilities Assessment and Threats and Vulnerabilities Identification

Source: developed by the author.

The suggested algorithm to assess risks and capabilities, to identify threats and vulnerabilities can be applied to various branches and spheres of activity. Still, any assessment of resilience of society, communities, critical infrastructure, organizations and businesses has certain peculiarities. In this context, recommendations defined by international standards on resilience and sustainable development of communities, resilience of organizations and business process continuity, and others should be taken into consideration (ISO 2016, 2017a, 2018c, 2019b, 2019c, 2019d).

2.3.3. Basic Methods of Research Used for Risk Assessment

Issues of methodology for assessment of processes and results in complicated systems are within the scope of numerous studies, among which papers by Van Gigch (1981a, 1981b), Churchman and Ratush (1959), Kharazishvili (2019), should be highlighted. According to these authors, the main assumptions constituting the presumable basis for the respective assessments can be described as follows:

- any identifiable result has to be assessed (as quantitative or qualitative);
- defining results subjected to assessment can never be separated from the definition of properties (features) that form the results;
- relevance of the data subjected to assessment stipulates their validity and relevance for the established goals.

According to Churchman and Ratush (1959), the main challenges of an assessment are as follows:

- *language*: the way to formulate the assessment results in such a manner that allows for them to be communicated without any misinterpretation of their content;
- *level of detail*: which and how many data need to be used for assessment depending on the designated purpose;

- *standardization*: defining the conditions under which the correctness and objectivity of the assessments are guaranteed;
- *accuracy and control*: the requirement to assess deviations and monitor results under different conditions.

Although comprehensive risk assessment has a complicated interdisciplinary nature, it is still possible to identify the most common ***research methods*** used currently in the national risk assessment systems.

Environment statistical modeling which, when using the methods below, allows for:

- analyzing (within historic time dimension) interrelations between the periodicity of crises, first of all, natural disasters, changes of their features and consequences based on the *observation method*;

- anticipating potential nature of risk manifestations on the grounds of identified regularities and limit value analysis, as well as for evaluating economic and other losses based on the *extrapolation method*.

Within statistical modeling of environment, crises of the past, which tend to repeat in cycles, are studied and compared with peculiarities of the contemporaneous security environment development; combinations of risk manifestations are simulated. Based on the respective analysis, a quantitative evaluation of the forecasted impact of crises is prepared for the case of their recurrence (financial losses, scale of infrastructure destruction, human losses, etc.) For calculation purposes, official statistical information and results of subject-matter analytical studies are used.

Crisis consequence modeling software. Computer simulation of disasters allows for simulating a large number of hypothetical crises on the basis of their random and unpredictable pattern. Digital catalogues of the simulated disasters including scenarios of emergency and other crises and numerical parameters of their consequences are generated. A series of risk manifestation scenarios are developed and prioritized. Such a methodological approach is based upon *probability theory* and *mathematical statistics*.

Risk assessment through consultations and decision-making process by a wide group of experts in the format of subject-matter sessions, inter-agency working groups, scientific conferences, etc. The most common are *Delphi technique* and *Cooke method*. Both methods provide for the creation of a subject-matter experts' group where each one of them is given an opportunity to independently assess the risks likelihood and impact, as well as to outline their manifestation uncertainty range. Further on, the outcomes produced by the experts' group are analyzed and the weighted average is deducted. To assess crises` likelihood and consequences, *an objective calibration method* is applied, where each one of the experts defines the highest, medium, and lowest limit values of the risks likelihood and impact according to the elaborated parameters.

Application of correction factors to the quality of the involved experts allows for reducing the level of subjectivity and for increasing the level of assessment and forecast confidence level. Peculiarities of defining accuracy and reliability of expert's forecasts are characterized, in particular, in the works by Van Gigch (1981b).

In general, according to the world experience, national risk assessment systems use different combinations of the aforementioned research methods.

2.3.4. Generation of Threat Data Sheets and Registers

Threat Data Sheets (Threat Passports) and Registers are a user-friendly form to systemize strategic analysis results, which are used for planning and adaptive management in national security. Their availability facilitates continuous situational monitoring in the national security field and contributes to timely corrections of the national policy in relevant directions and of any specific measures related to it.

According to Ukrainian researchers Sytnik, Abramov, Mandarelya, Shevchenko and Shypilova (2012), Threat Data Sheet (Threat Passports or Matrix) is a document to identify (assess) events, phenomena, processes, and other factors posing risk to the implementation of critical national interests of Ukraine, to characterize further evolvement thereof, as well as to define basic institutional, legal, and other mechanisms with respect to activities of the national security actors responding to threats. The practicability of drafting such documents and creating the respective databases has been stressed also by Bohdanovich, Semenchenko and Yezheyev (2008).

Taking into account opinions expressed in the respective scientific literature, the format of Threat Data Sheet could be suggested to consist of *three main parts*:

- Part One would contain *threat characteristics*;
- Part Two would define *the capabilities required to respond to the threat;*
- Part Three would contain *protocols of concerted actions* concerning response to the threat (Reznikova, 2018e).

The threat characteristic provided in the first part of the Threat Data Sheet allows for identifying certain events and/or phenomena as a threat according to pre-established criteria; defining the configuring factors thereof; any factors (events, phenomena, or processes) contributing to manifestation thereof; potential consequences for the national security, target groups, etc.

The second part of the Threat Data Sheets identifies the institutional and legal mechanisms and the authorized state bodies` resources required to adequately respond to the threat with respect to the stages of the national resilience ensuring cycle. To generate the first two parts of the Threat Data Sheet, results of the comprehensive risk and impact assessment and of the capabilities review mentioned in this monograph above have to be used.

Timely generation and implementation of the universal protocols of concerted actions for the threat response, which constitute the basis of the third part of the Threat Data Sheet allow for conducting targeted exercises and trainings where skills and culture of overarching interaction are developed and shortcomings requiring correction are found. This fosters an increase in the state's and society's level of readiness to respond to threats and crises.

Analysis of the security situation and capabilities condition conducted on the basis of the completed Threat Data Sheets gives the national security and resilience actors an opportunity to identify dangerous trends and impact factors and weaknesses in their activities and interactions with other actors and to make timely corrections in the action plans.

Completion of *the National Risk Register* has become nowadays a common practice around the world, which is used, in particular in the United Kingdom, the Netherlands, New Zealand, and other countries. Expanded versions of such Registers contain summarized results of the comprehensive risks and capabilities assessments, identification of threats and vulnerabilities, as well as conclusions and recommendations for development of the national policy including the area of national security and resilience, which is not disclosed to the public. Besides, they are an important tool for planning security and resilience measures at all levels (national, regional, and local).

Shortened publically accessible versions of such registers are an important tool to increase public awareness concerning the security situation, relevant threats, and mechanisms to respond to them, first of all, from the point of view of the interaction between the public and national and local authorities. In view of the results of the world experience analysis, the National Risk Register can comprise three main parts:

1) general characteristic of the current security situation and trends of its evolution, as well as threats to the national security and consequences of their manifestation requiring the most attention;

2) brief characteristic of each one of the high priority threats and crises, which contains:

- description of threat manifestations and potential their impacts;
- outline of the responsibilities and procedures of response by the national and local authorities;
- information for the public concerning the emergency procedures aimed at making them, their relatives, properties, etc., safe to the maximal extent possible;
- important contact points of the authorized national and local bodies and references to useful web-resources;

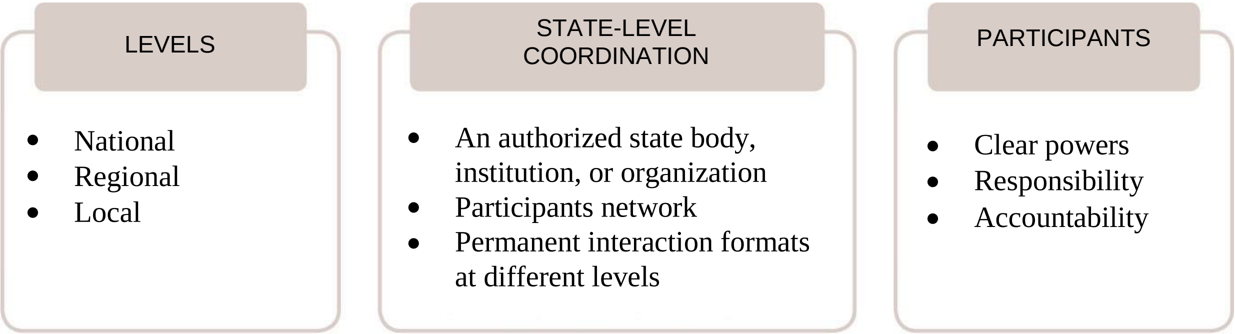
3) description of the methodology used to complete the Register.

It should be added that the countries included in this study have an identified public authority or institution responsible for preparation, completion, promulgation and periodic update of their National Risk Registers. The Public Register is placed on the official web-site of such public authority/institution or on a special page of the Governmental Information Portal. Based on the National Register, regional risk registers can be prepared where both the overall national situation and regional peculiarities are considered. Hence, preparation of the national and regional risk registers promotes an increase in the readiness levels of various actors for potential threats and crises of a wide spectrum, generation of common approaches to the threat identification, enhancement of efficiency of inter-agency interaction in the national security, etc.

2.3.5. Institutional Support to National Risk Assessment System

The efficient functioning of the national risk assessment system depends on the respective its legal and institutional support. The main principle of such system's organization is wide inter-agency cooperation. The relevant systems can be created and operated at both national and regional or local levels.

Usually, national legislation defines a public authority or an institution responsible for coordination of activities in the risks and threats assessment and for keeping the national risk register, as well as powers, responsibilities, and accountability of the involved public and local authorities, institutions, and organizations. General characteristics of the national risk assessment system organization are presented in *Fig.2.5.*



LEVELS

- National
- Regional
- Local

STATE-LEVEL COORDINATION

- An authorized state body, institution, or organization
- Participants network
- Permanent interaction formats at different levels

PARTICIPANTS

- Clear powers
- Responsibility
- Accountability

Fig. 2.5. Peculiarities of National Risk Assessment System Organization

Source: developed by the author.

There are also examples of the use of an informal approach to the organization of risk assessments in the state. For instance, in Switzerland, sectorial and regional authorities submit on voluntary non-regulated basis information necessary for the central government to make their assessments and conclusions. Such an approach can be effective only in the case when such activity is an element of the overall national policy in national security and resilience and an appropriate inter-agency culture has been developed in the state.

Creation and functioning of the national risk assessment system are especially important on the initial stage of the building up of national resilience when the appropriate culture and political and managerial processes are at the stage of their development.

Now, in most countries, the governments determine the general procedure of national risks and threats assessment, control the respective process, and establish the regulations concerning access to the results of such efforts. In such assessment, the leading role belongs to an inter-agency working group comprised of representatives of authorized ministries and agencies. Scientific research institutions and independent experts can be involved in this effort. Thus, in the Netherlands, to assess risks, the National Network of Safety and Security Analysts comprised of experts from governmental research centers, academic institutions, and the private sector has been established. In the United Kingdom, Natural Hazards Partnership is engaged.

According to the world experience, the most effective are risks and threats assessment multi-level systems, when the appropriate analysis is conducted at national, regional and/or local levels. Such practices are common for the states with well-developed inter-agency cooperation and interaction mechanisms at the regional level and with sufficient decentralization level in the national security sphere. For purposes of comprehensive risks and threats assessment, regional networks involving representatives of local and national authorities in the regions, communities, regional research institutions and organizations, etc. are created. Such regional networks develop regional risk registers on the basis of national overarching recommendations with due consideration of the results of the assessment conducted at the national level. In particular, the United Kingdom involves in this effort the Local Resilience Forums and in the Netherlands – the Security Regions.

The aspects of substantial importance that require special attention in the process of organization and ensuring functioning of the national risk assessment system are presented graphically in Fig. 2.6.

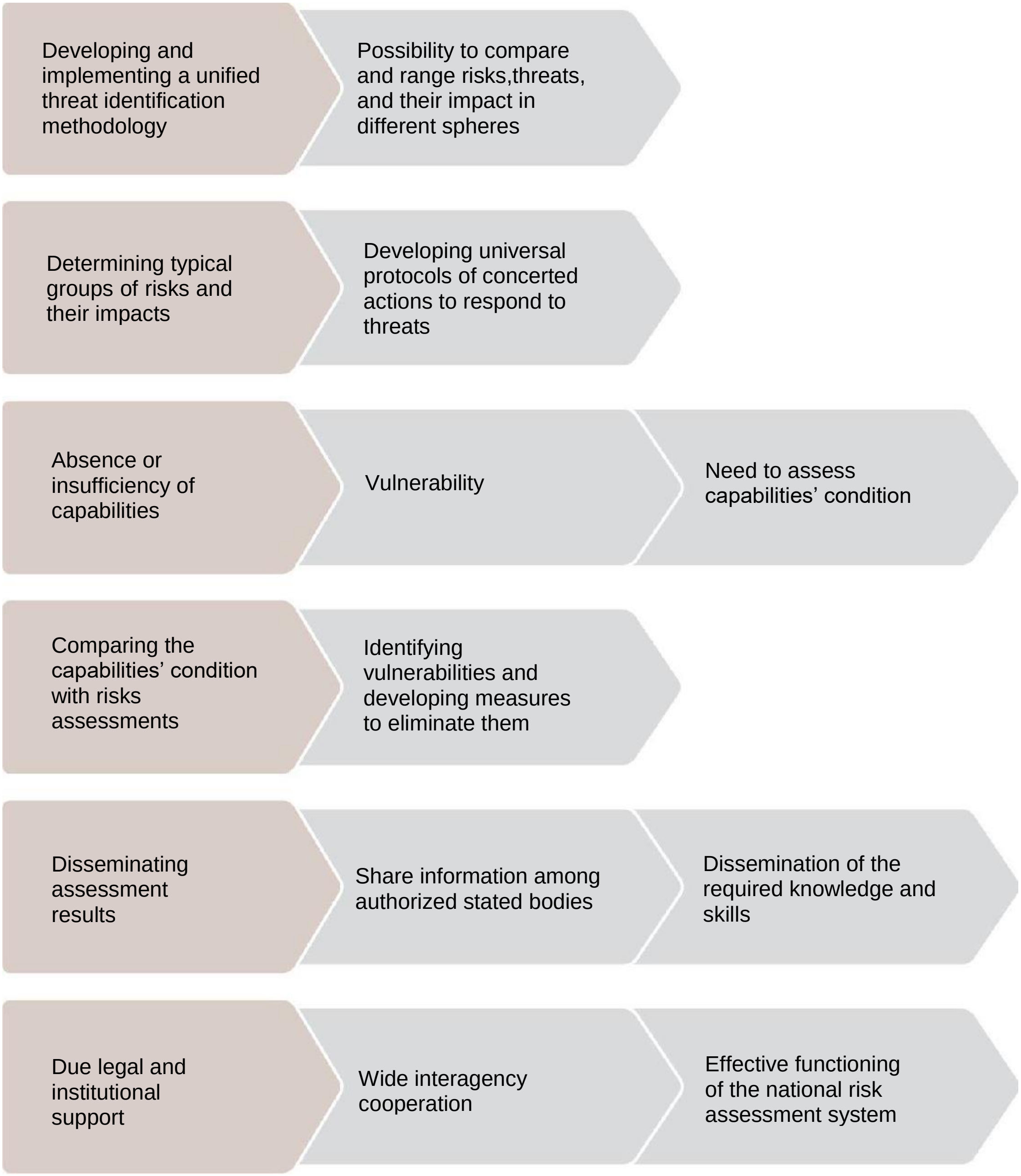

Developing and implementing a unified threat identification methodology
Possibility to compare and range risks,threats, and their impact in different spheres
Determining typical groups of risks and their impacts
Developing universal protocols of concerted actions to respond to threats
Absence or insufficiency of capabilities
Vulnerability
Need to assess capabilities' condition
Comparing the capabilities' condition with risks assessments
Identifying vulnerabilities and developing measures to eliminate them
Disseminating assessment results
Share information among authorized stated bodies
Dissemination of the required knowledge and skills
Due legal and institutional support
Wide interagency cooperation
Effective functioning of the national risk assessment system

Fig 2.6. Aspects of Essential Importance in Organization and Functioning of National Risk Assessment System

Source: developed by the author.

OECD (2017) underlines, among *issues* related to the creation of a national risk assessment system in many countries, the following challenges: lack of qualified personnel; methodological flaws which can lead to underestimating or overestimating certain risks; an increase of unpredictability of the future; difficulties in measuring national resilience level and conducting review of capabilities; limited resources; lack of political will to implement such a system in the state, etc.

A comprehensive national risk assessment system is an important element to provide national security and resilience. It allows for practical implementation of the adaptive management model in the national security field under conditions of the uncertain and unpredictable global environment. At the same time, poor quality, superficial or biased analysis of the security situation, in particular, with respect to major threats to the national security, the state's and society's (including target groups) resilience to such threats, as well as an incorrect definition of the high priority measures, can result in the wrong or insufficiently grounded decision in the sphere of national policy. If the policy is viewed through the prism of the state's improvement as a complex system, then, according to Van Gigch (1981a), any activities grounded on wrongful results of the problem analysis (including analysis of preconditions for the their emergence and methods of their solution) can make the situation even worse than it was before the "improvement".

2.4. Multi-Level Nature of National Resilience Ensuring System

When describing levels of organization of the national resilience ensuring system, researchers, most commonly, identify the following ones: state, regional (within a state), local (territorial community level) as territorial levels, as well as object level (organizational resilience).

It was noted that the state in general and its separate regions in particular continuously face different kinds of risks, emergencies and crises that can destabilize or even change directions of their development (Reznikova, Voytovskyi and Lepikhov, 2021). At the same time, different regions, due to peculiarities of their geographic situation, historic, cultural, economic, and political development, etc. can have different vulnerabilities. The building of the regional resilience is important not only in the context of minimization of such vulnerabilities but also in order to solve any problems which impede sustainable development of regions within a single state.

Applying the systems approach to analyze the life conditions in modern circumstances, Van Gigch (1981a) focused on the following key matters of the national policy: *when* is it required for the state to interfere with regional matters?, *how* would such interference be correctly organized without restricting freedom of action at the local level? The scholar emphasizes that systemic problems require systemic solutions. In practice it means that in order to solve modern security problems when resources are limited it is necessary to find such a solution for a complex system which would not only meet the goals of subsystems but also ensure the global system's integrity. Such solutions need to be acceptable for all systems and for all individuals (Van Gigch, 1981a).

As Chapter 1 of this monograph defines, the key principles of national resilience include, inter alia, the wide interaction and subsidiarity. The subsidiarity means that threats and crises should be responded to at the lowest possible level with proper coordination at the highest reasonable level.

Development and implementation of the national resilience ensuring system require, among other, effective coordination and efficient interaction of the security and defense sector authorities, other public authorities, territorial communities, businesses, civil society, and the public in prevention of the threats, threat response and mitigation of the crises impacts, establishing and maintaining reliable communication channels between the public authorities and the population over the whole territory of the country, etc. To execute this task, it is necessary to organize cooperation and establishment of the required organizational mechanisms not only at the overarching national level but first of all, at regional and local levels. Organization of formats (entities) for the interaction of the central and local authorities, enterprises and organizations, the public and mass media which are in continuous operation, as well as the development of public-private partnership at the regional and local levels, is the necessary condition for effective implementation of the national policy in national security and resilience. Many countries of the world have operational comprehensive multi-level systems ensuring national resilience, and, among them, the most illustrative are examples of the Netherlands and the United Kingdom.

A review of the scientific literature and world experience allows for concluding that currently there is no single commonly recognized methodology for building the national resilience and community resilience, in particular, with respect to the way they need to be built and assessed. The main goals and objectives in this domain should be defined on the basis of conceptual foundations of building national resilience and an appropriate organizational model of its implementation in the state. It is also important to apply criteria of territorial community`s resilience, which then could be a mean to assess progress in achievement of the designated objectives.

Effective organization of the system ensuring the security and civil protection of the regions and territorial communities is extremely important to build the national resilience of any state. It is at the local level where the threats and crises are primarily responded to and contained. In view of this, the regions and territorial communities must have sufficient capabilities and reserves to respond to a wide spectrum of threats, to be prepared for inter-agency cooperation, interaction with the population, neighboring regions and public authorities. Graphic presentation of the need to ensure the resilience of the regions and territorial communities is given in Fig. 2.7.

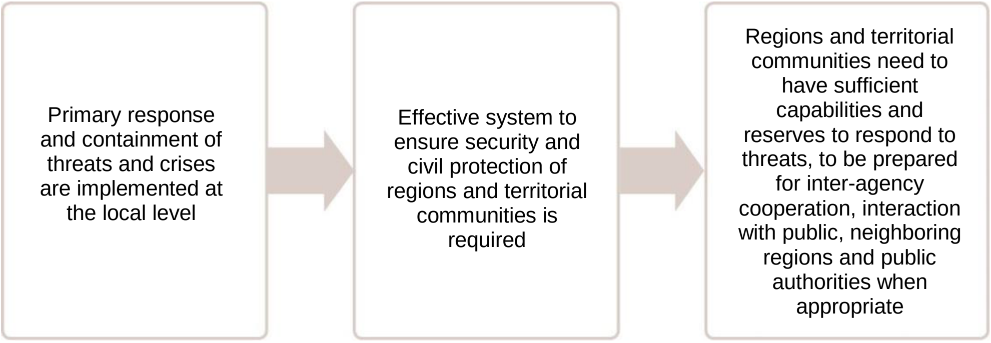

Primary response and containment of threats and crises are implemented at the local level
Effective system to ensure security and civil protection of regions and territorial communities is required
Regions and territorial communities need to have sufficient capabilities and reserves to respond to threats, to be prepared for inter-agency cooperation, interaction with public, neighboring regions and public authorities when appropriate

Fig. 2.7. Substantiation of the need to ensure the resilience of the regions and local communities

Source: developed by the author.

Peculiarities of resilience ensuring activities of the regions and territorial communities are determined by the relevant principles, goals, and objectives which should be based on the essential characteristics of the national resilience concept (*Table* 2.2).

Table 2.2

Peculiarities of the activities ensuring the resilience of the regions and territorial communities

Features of organization of activities	Content
Key Principles	• Legitimacy and continuity; • clear delineation of powers between central and local authorities; • interaction and cooperation; • responsibility; • awareness and reasonable transparency of activities.
Main Goals	• To form adaptive management model based on wide interaction; • to ensure cohesion of local communities; • to create joint capabilities of communities; • to improve planning in order to ensure proper level of preparedness and effective response to threats and crises; • to provide effective civil control.

Main Objectives	• To timely identify risks and threats; • To assess the appropriate capabilities; • To identify vulnerabilities; • To promote the required knowledge and skills; • To act proactively whenever possible; • To solve problems precluding sustainable development.

Source: developed by the author.

The following *principles* of organizations of resilience ensuring activities of the regions and territorial communities should be defined:

- legitimacy and continuity, which means to ensure the ability to make, explain and implement decisions even in crisis, as well as the need to fulfill decisions in a lawful, effective and accountable manner at any time;
- clear delineation of powers between the state and local authorities when responding to threats and crises of a pre-determined scale, origin, and nature;
- interaction and cooperation, which stipulates regular inter-agency meetings with participation of representatives of the regional and local authorities, civil society, business, mass media, etc.;
- responsibility of all resilience actors for providing preparedness to respond to threats and crises and for implementation of all pre-defined measures including joint activities;
- awareness and reasonable transparency of the activities in the sphere of ensuring the resilience of regions and territorial communities.

The main goals of ensuring the resilience of regions and territorial communities are:

- to generate an efficient governance model on the basis of a wide interaction (inclusion) with consideration of the adaptive management principles;

- to ensure cohesion of the local communities: unity around matters of providing their security and resilience;
- to create joint capabilities of a community including resource, institutional and social capabilities, etc.;
- to improve the planning with the purpose to ensure an appropriate level of preparedness and effective response to wide spectrum threats and crises;
- to provide effective civil control of the use of resources at regional and community levels.

According to conceptual framework of ensuring national resilience at the level of regions and local communities, it is necessary to timely identify risks and threats, assess the appropriate capabilities, identify vulnerabilities, disseminate the required knowledge and skills, prepare the required reserves, act, if possible, proactively, solve challenging issues that hamper the sustainable development.

In general, all resilience ensuring processes in the state have to run within a single cycle, be well coordinated at all levels, and meet the essential features of the national resilience. This foundation pinpoints the generation of the multi-level comprehensive model of ensuring the national resilience, which is graphically presented in *Fig. 2.8*.

Each country chooses its high-priority spheres, sectors, and mechanisms to ensure national resilience at its own discretion (the options suggested in *Fig.2.8* are the most common and not exclusive). No matter what has been chosen, clear distribution of powers between the central, regional, and local authorities, allocation of continuous communication channels and interaction mechanisms (including those between the neighboring regions) enhance the effectiveness of both primary response to threats and crises, and the functioning of the national resilience ensuring system in general.

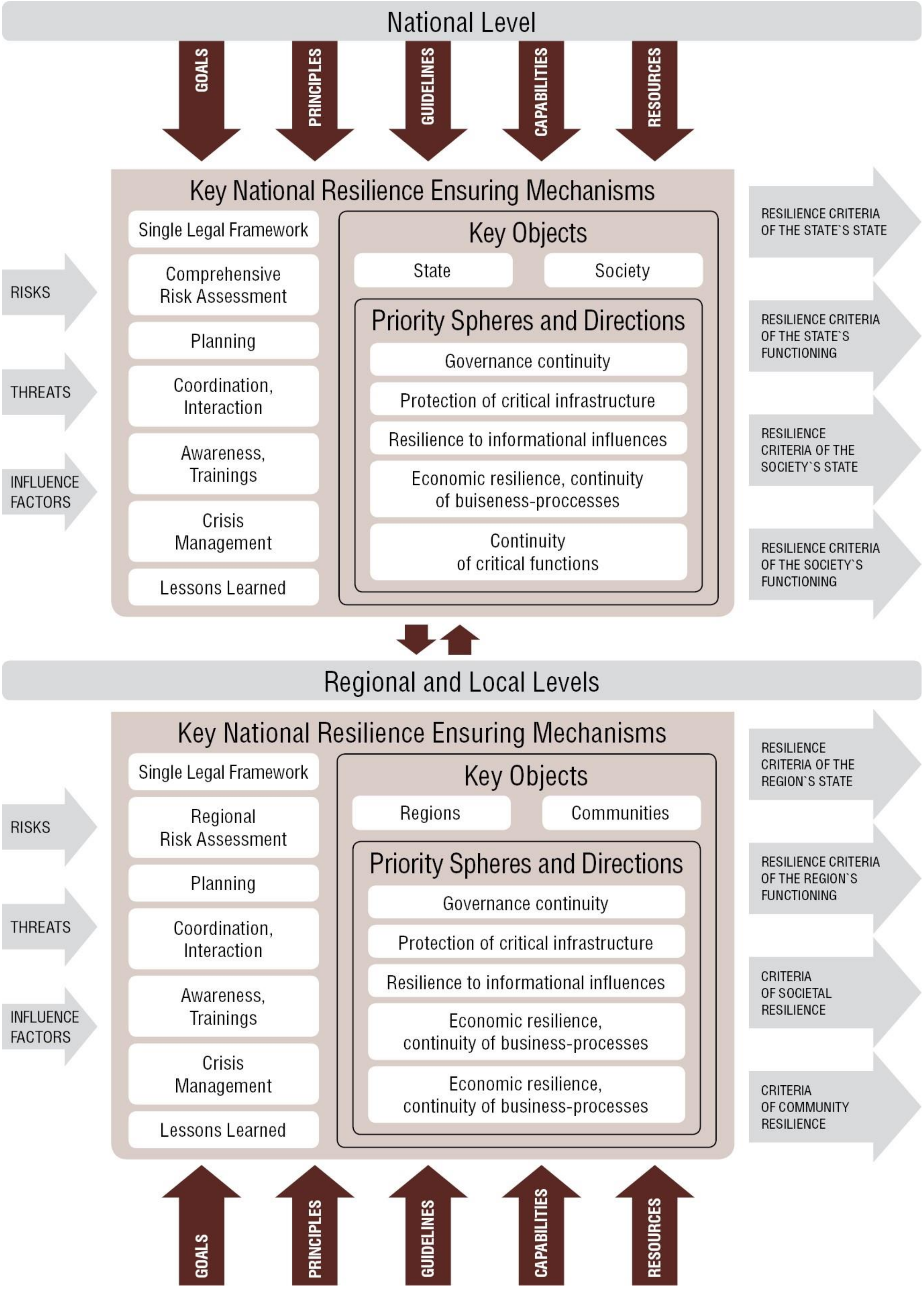

National Level
GOALS
PRINCIPLES
GUIDELINES
CAPABILITIES
RESOURCES
Key National Resilience Ensuring Mechanisms
Single Legal Framework
Comprehensive Risk Assessment
Planning
Coordination, Interaction
Awareness, Trainings
Crisis Management
Lessons Learned
Key Objects
State
Society
Priority Spheres and Directions
Governance continuity
Protection of critical infrastructure
Resilience to informational influences
Economic resilience, continuity of buiseness-proccesses
Continuity of critical functions
RISKS
THREATS
INFLUENCE FACTORS
RESILIENCE CRITERIA OF THE STATE`S STATE
RESILIENCE CRITERIA OF THE STATE`S FUNCTIONING
RESILIENCE CRITERIA OF THE SOCIETY`S STATE
RESILIENCE CRITERIA OF THE SOCIETY`S FUNCTIONING
Regional and Local Levels
Key National Resilience Ensuring Mechanisms
Single Legal Framework
Regional Risk Assessment
Planning
Coordination, Interaction
Awareness, Trainings
Crisis Management
Lessons Learned
Key Objects
Regions
Communities
Priority Spheres and Directions
Governance continuity
Protection of critical infrastructure
Resilience to informational influences
Economic resilience, continuity of business-processes
Economic resilience, continuity of business-processes
RISKS
THREATS
INFLUENCE FACTORS
RESILIENCE CRITERIA OF THE REGION`S STATE
RESILIENCE CRITERIA OF THE REGION`S FUNCTIONING
CRITERIA OF SOCIETAL RESILIENCE
CRITERIA OF COMMUNITY RESILIENCE
GOALS
PRINCIPLES
GUIDELINES
CAPABILITIES
RESOURCES

Fig. 2.8. Multi-level comprehensive model of ensuring national resilience

Source: developed by the author.

Conclusions to Chapter 2

To implement the national resilience concept, the theoretical and practical approaches to formulation of the state policy in national security need to be better specified. First of all, it concerns the role of the state and the re-distribution of powers in the field of national security and resilience. In the context of shaping effective systemic links, it is fundamentally important to find an optimal balance between centralization and decentralization of public administration functions in this sphere.

In the developing countries, especially at phases of transition and under conditions when an appropriate security culture has not been shaped yet, the state has a decisive role in ensuring national resilience. Still, the roles of other national resilience actors grow with time. From being merely entities executing separate functions entrusted to them, they turn into active actors in many processes. Having in mind that complex social systems (including society, territorial communities, institutions and organizations, enterprises, and public associations) have the ability to self-organize and to self-govern, it is important to make sure that such processes within the state are guided.

To implement the subsidiarity principle, which is one of the key principles to ensure national resilience, an effective primary response to threats and crises has to be in place, which requires creation or strengthening of local security capabilities, social capital, etc. in line with expanded powers of local authorities and territorial communities in the sphere of ensuring national resilience. In parallel, the state retains the leading role in solution of strategic issues of ensuring national security and resilience and the state’s overseeing and coordinating functions are strengthened. The suggested re-distribution of responsibilities in the sphere of national resilience contributes to the increase of the preparedness levels of the state and society, as well as of the regions and local communities, to respond to a wide spectrum of threats including hybrid ones. Also, it allows for taking into consideration peculiarities of regional development and for applying a resource-efficient approach to shaping the state policy in the respective area.

For the development and implementation of the state policy in national security and resilience, it is fundamentally important to define the general model of ensuring national resilience, key parameters, goals, and objectives thereof, peculiarities of shaping the mechanisms for adaptive management of resilience and new institutional formats of wide interaction, clear distribution of responsibilities among all the actors including those related to dissemination of the required knowledge and development of society's skills. At the same time, to develop societal resilience and community resilience, it is required to implement measures aimed at eradication of conflicts, building of unity around security issues, and creation of joint capabilities, as well as developing a sense of safety of the population and awareness of the action plan in case of increasing the level of certain threats, etc.

The goal of the national resilience adaptive management is to retain the main processes and parameters of the functioning of the state and society within the boundaries of dynamic balance. Maintenance of an optimal for the certain conditions level of resilience in specific spheres is an important task in generation of the state policy in national security and resilience because it sets a guideline for the functioning of the national resilience ensuring system, which need to be periodically reviewed with consideration of the timeframe and the general context of the situation. Also, under current conditions, the strategic analysis, as an inseparable part of the national resilience adaptive management, becomes very important. It allows for timely detection of dangerous threats in the security environment and vulnerability of the state and society, for adjusting the respective state policy and action plans and, when necessary, the national resilience ensuring model. Practical implementation of the goals, priorities and objectives designated by the state in the field of national resilience stipulates introduction of specifying corrections in the everyday activities of central and local authorities, shaping the unity, trust, leadership and security culture in the society.

Taking into account the conclusion concerning the compatibility of the national security ensuring system and the national resilience ensuring system, it can be noted that development and implementation of a comprehensive state policy in national security and resilience allows for enhancing its flexibility and adaptability to quick changes of the security environment on one hand and for increasing preparedness of the state and society to respond to a wide spectrum of threats including hybrid ones on the other hand.

According to the world experience, the national resilience ensuring model is defined by each country individually on the basis of such country's national interests, security environment peculiarities, participation in certain international organizations, alliances, etc. Hence, the priorities and mechanisms to ensure national resilience chosen by various states may differ while the practices that have demonstrated sufficient effectiveness in certain countries may fail to meet the security conditions and national interests of other states. Within the pre-defined national resilience ensuring model, respective systems of institutional and legislative support are built with consideration of the national legislation peculiarities, local traditions, etc.

Results of the analysis of the practical implementation of the national resilience concept demonstrate the advantages of implementation of the comprehensive approach to the providing preparedness and effectiveness of the response to threats of various nature and origin and quick recovery after the crisis, according to which matters of civil defense and crisis management are viewed together with other aspects of ensuring national security. With this, major importance is gained not only by inter-sectorial and inter-branch cooperation but also by an active interaction and partnership of the state and local authorities with the public and businesses within the pre-established responsibilities as a foundation that forms reliable systemic links.

Implementation of the systems approach to the ensuring national resilience called forth the implementation of universal mechanisms and measures aimed at a comprehensive response to a wide spectrum of threats and crises at all stages of the ensuring national resilience. In particular, what is meant here is the national system for risk and capabilities assessment, identification of threats and vulnerabilities; multi-level system of national resilience management; strategic analysis and planning system, etc. The national resilience ensuring system shaped in accordance to the pre-defined theoretical principles and regularities should not be static. In view of the fact that the threats to national security in the modern world have a complex and dynamic nature, the state policy in national security and resilience needs to be periodically specified while the aforementioned system needs to be complemented with new mechanisms and tools.

Chapter 3
A 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

[1] *Euro-Atlantic Disaster Response Coordination Centre*. https://www.nato.int/cps/en/natohq/topics_52057.htm

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 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

[2] *Civil Emergency Planning Committee*. https://www.nato.int/cps/en/natohq/topics_50093.htm

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), 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

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

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

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

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 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

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

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;
- 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

[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

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;
- 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.

[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

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.

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

[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

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, 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 of

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

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 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

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

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 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.

[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

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; 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.

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

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 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].

[17] *Wales Resilience*. https://gov.wales/wales-resilience/what-we-do

[18] *Preparing Scotland: Philosophy, Principles, Structure and Regulatory Duties.* https://ready.scot/

[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

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.

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].

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)

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

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.

Chapter 4
CURRENT SECURITY ENVIRONMENT AND THE STATUS OF NATIONAL RESILIENCE IN UKRAINE

The study of security environment, identification of dangerous trends, factors of influence, and risks and threats to national security allows for a well-grounded choice of an optimal national resilience ensuring model and the appropriate mechanisms for the state in the current conditions. However, a comprehensive analysis of existing capabilities, practices, regulations, and organization of activities in the field of national security, crisis management, and public administration helps to identify vulnerabilities and systemic challenges with regard to ensuring national resilience, as well as formulate the priorities in terms of its further enhancement. Analysis of these issues has a scientific and practical significance in the context of substantiating the expedience of creating a national resilience ensuring system in Ukraine, and identification of its key features, taking into account the identified regularities and essential characteristics of the national resilience concept.

5.1. Key Trends in Ukraine’s Security Environment

Ukraine’s security environment analysis is expedient to start by identifying the main processes and tendencies describing the *changes in global security environment* and shaping the contours of global development.

Most experts acknowledge that the global security environment is currently characterized by a high level of uncertainty and unpredictability. The US National Intelligence Council (2021) emphasizes that the Covid-19 pandemic reminded the world of its fragility and demonstrated the high interdependence of various risks. According to experts, in the forthcoming years and decades, the world can face more intense and cascading global challenges of different origins, which will be a test for resilience and adaptability of communities, states, and international system on the whole.

The subject publication highlights the following most probable risks and tendencies of global development:

- increasing political rivalry in the world and a greater risk of conflict, as states and non-state actors, exploit new sources of power and erode the long-standing norms and institutions that supported global stability in the past decades;
- increasing disparities in economic development and competition across global markets;
- unevenly aging populations offering demographic dividend to the developing countries in Latin America, South Asia, North Africa, and the Middle East;
- more intense effects of climate change;
- increasing social stratification in societies, growing distrust of power, forming groups of like-minded people based on an established or newly acquired identity;
- growing political instability in the states and erosion of democracy;
- greater threats from the accelerated development of cutting-edge and break-through technologies (US National Intelligence Council, 2021).

The UK Ministry of Defense (2018) notes that the world is becoming ever more complex and volatile, and “the only certainty about the future is its inherent uncertainty.” According to the experts of the UK Ministry of Defense, the rate of change and level of uncertainty may outpace the good governance and unity of societies. This requires adaptation, prevention, and active response to threats.

The experts identified the trends that will be observed over the next 30 years (until 2050) and will require adaptation:

- increasing human empowerment: development of novel knowledge and technologies, on the one hand, opens new opportunities in education and medicine, while deepening, on the other hand, the social stratification in societies, thus exacerbating political discord;
- power transition and diffusion: growing rivalries between Asian states (primarily China and India) and the USA, and also, competition between other states will require reform of international institutions. Not all states will be able to stand up to merging political and social challenges (UK Ministry of Defense, 2018).

Among the trends requiring prevention or mitigation of effects, the UK Ministry of Defense experts name the following:

- dramatically increasing role of information (centrality of information): people having broader access to information, development of computer technologies, artificial intelligence, digitization of numerous aspects of life, while enhancing human empowerment, these also create new risks associated with the potential polarization in societies due to social media, lower public confidence in existing government institutions, a surge in cyber-attacks and other crimes committed via the Internet and social networks
- accelerating technological advancement: development of advanced technologies in industry (the Fourth Industrial Revolution) has an impact on all sectors of economy and exacerbates the risks of social changes, public discontent, and protests due to job reduction and changes in their quality, and also aggravates working and leisure conditions for people (UK Ministry of Defense, 2018).

The UK's experts also defined trends that will require active response:

- a greater pressure on the environment as a result of climate change and human activities;
- disproportionate changes in the composition of population in different countries that may result in growing migration and increasing

pressure on social services system and infrastructure of certain towns, (UK Ministry of Defense, 2018).

According to the UK experts, those events and emergencies that cannot be foreseen are the greatest risks. These include, in particular, significant changes in the establishment of geopolitical alliances, sudden shifts in the social, economic or political paradigms, severe conflicts and natural disasters, financial crises, damage to global infrastructure, collapse of international organizations, (UK Ministry of Defense, 2018).

According to K. Friberg[23], Head of the Swedish Security Service, what is considered an opportunity today may pose a threat in the future, and the most important incidents are the ones that never happen. The expert emphasizes a much more complex character of contemporary threats versus the traditional ones.

The WEF (2021b) lists the following most likely global risks over the next ten years: extreme weather, climate change, human environmental damage, concentration of digital power, digital inequality, and cybersecurity failure. The risks that may have the most severe impacts include, in particular, infectious diseases, climate change and other environmental risks, proliferation of weapons of mass destruction, livelihood crises, debt crises, and IT infrastructure breakdown.

According to Smil (2012), in the next fifty years the greatest threat for humans is the possibility of a new mega-war that will have the greatest fatal consequences. Among other significant risks with comparatively lesser likelihood of occurrence and lesser impacts, the scientist names pandemics (primarily flu), volcanic eruptions, and tsunamis.

The World Bank (2012) points to the growing conflict potential and the consequences of potential violence outbursts for global security and development. The World Bank's experts provide cost estimates of losses that may be incurred by national economies and the global economy in the case of an armed conflict. D.H.

[23] The Swedish Security Service. *Annual Report 2020.* Retrieved from https://www.sakerhetspolisen.se/download/18.4ffee9b31787cb4eddc4ec/1624002656682/Swedish%20security%20service%20annual%20report2020.pdf.

Meadows, Randers and D.L. Meadows (2012) argue that the forecasts of global development need to consider the impact of risks associated with the existence of certain limits to growth, the continuous tendency of the world system toward growth, as well as the time lag between approaching the limit to growth and the society's response thereto.

Considering the enhancement of interconnections and interdependence between states, the scale of influence of global risks on national and international security will be increasing. The effectiveness of measures to prevent and address them will significantly rely upon the ability to identify and assess global risks. However, considering that a significant part of them is difficult to project with a high degree of probability, it is the enhancement of national resilience that appropriate prevention strategies should rely on (Reznikova, 2013a).

Official documents of international organizations and many countries mention the increasing level and scale of current threats. Thus, the Brussels Summit Communique, of 14 June 2021, notes that the Alliance and Member Nations face multifaceted threats, systemic competition from assertive and authoritarian powers, as well as growing security challenges from all strategic directions. The biggest threats to the world include Russia's aggressive actions, China's growing influence, illegal migration and human trafficking, the proliferation of weapons of mass destruction and erosion of the arms control architecture, hybrid, and other asymmetric threats, including cyber threats, disinformation campaigns, the malicious use of ever-more sophisticated emerging and disruptive technologies, (NATO, 2021a).

The Global Strategy of the European Union 2016 "Shared Vision, Common Action: A Stronger Europe" notes that the world lives in times of existential crisis. The document points to growing violence in various regions across the world, disproportionate economic growth, and climate change effects (European Union, 2016).

The United Kingdom's National Security Strategy and Strategic Defense and Security Review 2015 notes that in a rapidly changing, globalized world, what happens overseas directly affects internal security to a greater extent (UK Government, 2015).

Japan's National Security Strategy 2013 identifies the following challenges and threats to the global security environment: a shift in the balance of power and rapid progress of technological innovation; the proliferation of weapons of mass destruction and other related materials; international terrorism; risks to global commons (such as the sea, air and outer space, and cyberspace), related to the violation of international law and conflict of interests, challenges to the global human security and development (poverty, inequality, infectious diseases); risks to global economic development (Office of the Prime Minister of Japan, 2013).

The US National Security Strategy 2017 specifies that the world has become an extraordinarily dangerous place filled with a wide range of threats, including the proliferation of nuclear weapons, greater political, economic, and military rivalry between powers across the world, information campaigns to discredit democracy, radical terror groups, drug trafficking, and international crime, (President of the United States of America, 2017).

Analysis of the status of security environment and its development tendencies underpins the preparation of strategic documents in Ukraine. The National Institute for Strategic Studies [NISS] makes an important contribution in this effort by preparing annual analytical reports and other analytical documents for the leadership of the state. Thus, the analytical report of the National Institute for Strategic Studies to the Annual Address of Ukraine's President to Verkhovna Rada of Ukraine "On internal and external situation in 2020" notes that the world has entered into the times of dynamic changes, the result and behavior of which are hard to predict. Uncertainty and instability are the defining characteristics of today (NISS, 2020).

The National Security Strategy of Ukraine 2020 identifies the current and projected threats to national security and national interests of Ukraine with consideration of geopolitical and domestic circumstances. Among the threats related to global processes the focus is on the following: climate change effects and increasing human-led pressure on the environment; inequality and other fundamental disequilibria of global development; the growing international competition; implications of rapid technological shift; expansion of international terrorism and international crime; intensifying challenges to transatlantic and European unity that may lead to the escalation of existing and the emergence of new conflicts. As mentioned in this document, the on-going armed aggression of Russia against Ukraine, as well as Russia's *hybrid warfare* in the world, are the biggest threats to Ukraine (President of Ukraine, 2020b). Therefore, these threats affect the global security environment by aggravating it, and at the same time, they are sources of long-term destructive impacts on the national security of Ukraine.

Studying the specifics of hybrid warfare, including through the example of Russia, Rácz (2015) distinguishes the following its operational phases: preparation, attack, and stabilization. The scientist also notes that during the first phase the adversary usually puts together a "map" of strategic, political, economic, social, and infrastructure weaknesses and vulnerabilities of a victim-nation and creates the required mechanisms for their capitalization for further use. Such a period might last years and decades. Taking as an example Russia's aggression against Ukraine, Rácz (2015) concludes that during the initial phase it was practically impossible to determine whether Russia's actions, including those taken within the framework of traditional diplomacy, application of soft-power measures, external influence, were preparations to the hybrid warfare until an active phase (attack) began. This scientist believes that the following operational factors were drivers of effective hybrid aggression of Russia against Ukraine: suddenness, non-recognition of intervention at an official level, and occupiers' disguise as civilians. In addition, this was fostered by the lasting shared history of the two nations, close economic relations, as well as connectivity of political, business, and security sector elites (Rácz, 2015).

The above analysis of official documents and expert opinions regarding the current trends of global security environment development underscores *the* *difficulty of threat identification and risk assessment nowadays* (Reznikova, 2019b). Thus, the distribution of deceitful information to unroll destructive processes in society may be interpreted by the aggressor as freedom of speech and diversity of opinions. Organization of international conferences or other public discussion forums, where a new historical retrospective of the victim nation is "scientifically justified," and certain political events are explained to the benefit of the aggressor, may look like the "enhancement of scientific and cultural cooperation" between states. The attempts to have a direct influence on public opinion by spreading the aggressor's propaganda and justifying it are represented under the slogan of the freedom of media. The quite legal mechanisms, which rely upon traditional values, are used for this kind of activity. The "green men," who initially appeared in the Crimea and later in Donbas, were the subject of discussion in most countries across the world about whether or not this posed a threat to national and regional security and the way it should be responded to.

In the environment of hybrid warfare it is not only difficult to identify certain events or tendencies as a threat but also, to see a general picture behind them that may indicate that the adversary is preparing for more massive actions and is shifting to an active phase. Hybrid warfare involves a set of simultaneous massive and coordinated measures across various areas, including possible development of cascading effects. In today's world, economic, political, social, and other processes have strong inter-influence. That is why merely military methods often play a secondary role in hybrid warfare, while an aggressor uses destructive influences on economy, energy, information sectors, and society of a victim nation and other non-military tools as weapons. Initial identification of indicators of hybrid warfare requires certain time and coordination of effort between various state authorities.

The hybrid aggression of Russia against Ukraine highlighted the European security crisis. At the same time, as is noted by OSCE (2015), there is neither a shared idea, nor a general analysis of the situation regarding its causes and mistakes that were made in the course of its development, and the views from

Moscow, the West and states in-between differ considerably (OSCE, 2015). This proves the conclusion that there is a conflict of interests in the international arena and there is intensifying rivalry between states.

Ukraine has experienced to the full extent the on-going global changes. The hybrid warfare, launched by Russia in 2014, has radically changed Ukraine's security environment. The Russian aggression has practically affected all spheres of activities. This said, the flaws in domestic and foreign policy, ineffective institutions and mechanisms guaranteeing international security have had their effects resulting in the emergence of certain vulnerabilities of the Ukrainian state.

At the start of Russia's hybrid aggression against Ukraine in 2014, the national security system was apparently not prepared to respond to the emerging challenges and threats for various reasons, the senior leadership of the state left the country, security and defense agencies were not sufficiently effective, and the resources were catastrophically lacking (Horbulin, 2017). However, the civil society stood up to defend the national interests of the state, undertaking provisionally the important functions in the area of national security. The mechanisms of spontaneous self-organization entailing huge resilience potential of the state and society as complex systems were implemented in this manner. However, the adaptive governance mechanisms were underdeveloped at the time. In this regard, the role of civil society in nation-building processes has been downgrading in recent years, thus having a negative impact on the national resilience development.

While building up the joint effort format of countering the current security threats, including the hybrid ones, and reinforcing its own resilience, NATO focuses on the enhancement of cooperation with partner nations. In this regard, as a result of the NATO Summit in Wales in 2014, a decision was taken to provide assistance to Ukraine to support appropriately national security in the face of Russia's aggression (NATO, 2014). Thus, the NATO-Ukraine Commission meeting during the Summit meeting of NATO Heads of State and Government (held on 4 September 2014 in Newport, the United Kingdom) resulted in the

NATO Trust Funds establishment to support Ukraine, including in the following areas:

- modernizing command control, communications and computers structures and capabilities;
- reform of logistics and standardization systems of Armed Forces of Ukraine;
- enhancement of Ukraine’s cybersecurity capabilities;
- countering improvised explosive devices, explosive ordnance disposal and demining, (President of Ukraine, 2015d).

The decision to establish the NATO-Ukraine Platform for identifying lessons learned from the hybrid war in Ukraine, taken at the NATO Summit in Warsaw (9 July 2016, Poland), became recognition of Ukraine’s unique experience of responding to the hybrid aggression of Russia. This was one of forty areas of Ukraine – NATO cooperation within the framework of the Comprehensive Assistance Package for Ukraine, approved by the NATO Summit in Warsaw (NATO, 2016c).

The leadership of Russia has changed its rhetoric concerning Ukraine. Thus, in the recent national security strategy of this state that was approved on 2 July 2021 (President of the Russian Federation, 2021), Ukraine is mentioned just once, in contrast to the previous version, in the context of a strategic goal of the Russian Federation of “strengthening the fraternal ties between the Russian, Belorussian, and Ukrainian people,” rather than a neighboring state. Considering Russia’s apparent aspiration to take the leading role within the “new architecture of world order with new principles and rules,” which is repeatedly mentioned in this document, one should not count on the cessation of hybrid aggression against Ukraine. Rather, we should expect some changes in the methods of its conduct.

The subject document also emphasizes that nowadays the world goes through transformations, with the number of economic and political development centers going up, and new global and regional leader nations emerging. All of this comes amid the escalating instability in the world, geopolitical tensions, and conflict intensity.

In view of the long-term nature of the Russian threat and global security uncertainty, the *strengthening of national resilience as a strategic goal fully corresponds to the national interests of Ukraine*.

However, Ukraine's security environment is not just shaped by external threats and global trends. There are also a number of vulnerabilities in the state and society due to certain gaps in the organizational and legal support of processes that are going on in security area, as well as other factors.

For instance, Ukraine's National Security Strategy 2020 identifies threats from the Russian occupational administrations and armed forces of the Russian Federation across temporarily occupied territories in the Autonomous Republic of Crimea and the City of Sevastopol, and some areas of Donetsk and Luhansk regions of Ukraine, intelligence and sabotage operations of special services of other countries (primarily Russia) and destructive propaganda and disinformation. The following sources of threats to Ukraine's independence, sovereignty, and democracy have been specified, such as insufficient effectiveness of state authorities, thus challenging the development and implementation of effective state policy; low pace of rearmament of Ukraine's Armed forces and other forces of national security and defense sector on the advanced (upgraded) systems; inconsistent and uncompleted reforms, corruption; insufficient property right protection, extremely high proportion of the state's presence in the economy; insufficient level of competition and domination of monopolies, low energy efficiency; low level well-being of the population, radical moods in communities, rising crime rate; deterioration of critical infrastructure and the living environment; demographic challenges (President of Ukraine, 2020b).

It should also be noted that the character of some traditional threats is also changing. For instance, terrorist threat currently reshapes at both global and national levels and can be used as an element of hybrid warfare. It may affect regular functioning of the state and society. In general, armed violence and terrorism have a destructive impact on the development of any nation, hindering its economic growth and destabilizing society (Reznikova, 2017).

In addition, the character of separatist threat changes in current conditions. In Ukraine, for instance, indications of hybrid separatist conflict in Donbas, the underlying cause of which is political separatism, as inspired and actively supported by Russia, can be observed (Reznikova & Driomov, 2016). Thus, as we can see, the issues of internal and external security intersect more frequently.

Therefore, *the current security environment in Ukraine is characterized by a high level of uncertainty, considerable influence of global processes and trends, existence of a number of pending problems faced by public administration and national security system*.

The biggest *external threats* to Ukraine's national security include the on-going long-term hybrid aggression of Russia, increasing rivalry between states, and proliferation of weapons of mass destruction. The implications of these threats can be very dangerous: from the spread of disinformation, damage to critical infrastructure and essential services to population, to massive human and material losses, violation of the national sovereignty and territorial integrity of Ukraine.

Significant risks of the deployment of emergency and crises in Ukraine can be triggered by climate change effects and accelerated development of novel and cutting-edge technologies, potential spread of epidemics in humans and dangerous diseases in animals, contamination of environment, including water supply sources. Yet certain risks can evolve into threats to the national security of Ukraine or trigger new development opportunities. This primarily concerns the science and technology development potentialities.

The above risks and threats have a dynamic and long-lasting character, and they can cause major negative consequences for society and the state, and, aside from that, they cannot be eliminated fully.

In Ukraine, the *factors of influence and vulnerabilities that might aggravate security situation and affect the response to threats,* also include a number of important reforms that have not been completed (including in the sphere of national security and anti-corruption); a lack of resources (primarily financial) and their ineffective usage; a difficult demographic and social situation; a lack of competence of state and local government representatives; low public awareness regarding the existing and potential threats and hazards; a lack of public trust in state authorities.

Yet, there are a number of *factors strengthening the potential of national resilience i*n Ukraine. These primarily include developed legislation and institutions in the sphere of public administration and national security, the specifics of national mentality, such as aspirations for freedom and justice, high general level of educated population, the availability and accessibility of media and other sources of information.

In view of the character of key risks and threats to national security of Ukraine and concerning the specifics of national resilience concept implementation in the sphere of national security, as identified in Chapters 1 and 2 of this monograph, it may be concluded that *in a changing security environment, the introduction of systemic national resilience ensuring mechanism meets Ukraine's need to establish additional opportunities for ensuring national security in the context of comprehensive response to risks and threats of any nature or origin based on overarching cooperation*. The focused handling of identified problems, and vulnerabilities, reinforcement of existing advantages and buildup of national resilience mechanisms require an appropriate public policy formulation and implementation, including definition of goals and objectives in the subject domain.

5.2. Current Status of Providing Resilience in the Sphere of Ukraine's National Security

The very fact that Ukraine keeps existing and functioning as an independent state in the challenging environment, including armed aggression and crises of various origins, is evidence of a considerable resilience potential embedded both, in existing state institutions and mechanisms, and in society. However, there are a number of existing problems hindering the development of this potential. The key challenge in the sphere of ensuring national resilience is that relevant measures are fragmentary and non-systemic in their nature, and therefore, less effective. The absence of generally accepted terminology and conceptual distinctness with regard to ensuring national resilience, as well as imperfection of appropriate legislation, and a lack of well-tuned cooperation in this area – all of these altogether significantly impede the strengthening of national resilience and defy the key principles of its ensuring (comprehensive approach, broad cooperation, adaptability, predictability, reliability, awareness, preparedness, mobility, redundancy, continuance, and subsidiarity).

In addition, national resilience ensuring in Ukraine on a systemic basis is hindered by low level theoretical elaboration on the relevant issue. Presently there are too few researches concerning methodology for this process, its mechanisms, links to national security. In turn, this leads to inconsistent understanding of the concept of resilience in the sphere of national security, and difficulties with drafting new legislation.

Analysis of the general status of ensuring resilience in the sphere of national security of Ukraine should be completed in the context of national resilience ensuring cycle following the key phases, as proposed in Chapter 1 of this monograph. The main benefits and gaps of the relevant processes in Ukraine are described below, according to the subject approach.

Assessment of risks and capabilities and identification of threats and vulnerabilities.

In general, measures in the relevant areas are implemented by various ministries, agencies, and scientific institutions. Thus, according to the Law of Ukraine "On National Security of Ukraine," the National Security Strategy of Ukraine is duly prepared, where the current and projected threats to Ukraine's national security and national interests of Ukraine are described with reference to geopolitical and domestic conditions, and a comprehensive security and defense sector review is carried out (Law of Ukraine, 2018). While developing strategies in the areas of national security due to the subject Law and the National Security Strategy of Ukraine, the ministries and agencies shall carry out strategic analysis in their areas of responsibility and identify the specific risks and threats.

In addition, according to par. 68, National Security Strategy of Ukraine 2020, the National Institute for Strategic Studies prepares annual reports on the state of national security of Ukraine, based on the Strategy implementation progress analysis (President of Ukraine, 2020b). The analytical report of the NISS to the Annual Address of the President of Ukraine on internal and external situation of Ukraine to the Verkhovna Rada of Ukraine 2020[24] provides a detailed description of the current status of society and the state, including in the spheres of foreign policy, social relations. Analysis of these and other documents facilitates the identification of key vulnerabilities in society and the state.

At the same time, Ukraine faces essential problems of methodological and organizational character in the sphere of risks and capabilities assessment and identification of threats and vulnerabilities, and it also lacks an integrated theoretical and methodological framework to assess risks for national security and evaluate appropriate capabilities to prepare, adopt and implement strategic decisions; there is no public authority responsible for coordination in this sphere; there are gaps in information sharing in support of state decision-making processes.

Strategic analysis, prioritization in the area of ensuring national resilience, planning of measures to respond to the broad spectrum of threats, crises, and recovery thereafter. Specific national resilience ensuring objectives have only appeared in strategic documents and policies in recent years. No goals or objectives had been set by the state before. Presently no national resilience assessment indicators exist, and no guidelines regarding the definition of benchmarks, criteria, and mechanisms in this appropriate area have been developed, thus hindering objective identification of national resilience ensuring

[24] National Institute of Strategic Studies [NISS]. *Analytical report to the Annual Address of the President of Ukraine.* Retrieved from https://niss.gov.ua/publikacii/poslannya-prezidenta-ukraini.

priorities based on strategic analysis results. There is no systemic approach to the formulation and implementation of national resilience ensuring measures, which affects resource efficiency.

Uncertainty of the institutional model of ensuring national resilience in Ukraine and unresolved issues regarding the distribution of powers create numerous problems in the organization of relevant activities.

The formation of action plans to respond to threats and emergencies identified by law is carried out by various ministries and agencies in the prescribed manner. However, there is a range of problems in the area of joint efforts planning and setting out universal protocols of concerted actions, distribution of responsibility, and coordination of appropriate activities.

Another problem is that not all strategic planning documents accommodate the development alternatives, which reduces the level of adaptability of society and the state.

Ensuring preparedness and response to threats and emergencies identified by law is in the manner prescribed by relevant regulations. The main problems reducing the effectiveness of appropriate measures are as follows:

- lack of cooperation and coordination between various ministries and agencies;
- technical, moral, engineering, and material obsolescence of alternate control centers of public authorities;
- ineffective generation of necessary reserves by the state, including material and personnel;
- insufficient level of preparedness for joint response and collaboration between the state and local authorities and the population in case of threats or crises;
- low effectiveness of reforms in the country, corruption, ineffectiveness of a number of public services;

- inadequate level of public and community awareness regarding the nature of threats and response to crises;
- lack of bilateral channels of communication and poor communication between the state and local authorities and the public;
- low level public-private partnership in security area;
- inadequate level of population and public associations' involvement in the implementation of national security and resilience ensuring measures;
- low level of public trust in state authorities;
- lack of the government's focus on building national cohesion and culture of safety;
- insufficient effectiveness of governance in local communities.

A vivid example of the lack of preparedness to respond to threats was the poor technical condition of shelters and early warning alarm systems when Russia's aggression against Ukraine began in 2014.

The improper mechanisms of organization and coordination of actions in the sphere of crisis management at national, regional, and local levels pose considerable risks to ensuring the vital functions of the state and society under uncertainty and rapidly changing security environment.

The ability to prompt mobilization of efforts and assets during a crisis is still insufficient in Ukraine. This is primarily due to the inertia of the bureaucracy and the need for additional time to stage anti-crisis activities, especially in cases where the procedure was not determined in advance, which was confirmed in response to the spread of COVID-19 and the Russian occupation of Crimea. Information needed for decision-making is not always effectively shared between authorized bodies in crises.

Another problem in present-day Ukraine is an insufficient level of self-governance in society and the lack of self-regulated organizations capable of performing specific functions of public administration in crises in case of disorganization or failure of certain public administration elements (Reznikova, 2013b). For a long time, self-regulating organizations were predominantly represented in the financial market, i.e. stock market traders' associations, bank associations, associations of insurers. Yet, the role of trade unions in the employment market and social security regulation is still insufficient. Despite the boost in civil society development and the establishment of non-governmental organizations in Ukraine in 2014, when the mechanisms of spontaneous self-organization of society came into action in response to Russia's aggression, no effective mechanisms of directed self-organization have been created in Ukraine yet.

The process of post-crisis recovery of Ukraine and its regions tends to be complex, resource-consuming, and lasting. Thus, at the beginning of Russia's aggression against Ukraine in 2014, there were significant difficulties with accommodation and social support of internally displaced persons (IDP's) from temporarily occupied territories of AR Crimea and parts of Donetsk and Luhansk regions, and no solutions were provided for quite a long time (Kaplan, 2016). Floods in Transcarpathia, which occur almost every year, take lives and destroy infrastructure for billions of hryvnias, despite the fact that the authorized bodies of state power and local self-governments are implementing anti-flood measures.

Complex protracted recovery processes are observed in Ukraine after economic crises. According to Libanova (2020), the poor population benefited the least from the process of recovery of the national economy and suffered the worst from economic hardships. The scientist believes that a positive effect of economic growth in 1999–2019 allowed for a significant reduction of absolute poverty scale in Ukraine, while relative poverty rates remained practically unchanged because the income stratification could not be stopped. The scientist also states that currently Ukraine is one of the poorest European countries with a rather high level of poverty, and employment in Ukraine does not save the family from poverty (Libanova, 2020).

The above situations point out the existing systemic problems with national resilience ensuring in Ukraine, mostly in the area of ensuring continuous governance and provision of critical functions for the society, economic and social resilience.

Lessons learned. There is an established practice in Ukraine concerning learning and applying the sector-specific experience acquired by ministries and agencies through exercising and training (including international training) and other joint events in the area of national security, including with NATO and other international partners. Thus, joint events involving the Armed Forces of Ukraine are determined in Ukraine-NATO Military Committee Work Plan. The results of each of these are analyzed and considered in the planning of forthcoming events and programs. According to the official statement, eight multi-national exercises were scheduled to take place in Ukraine in 2021, with close to twenty-one thousand Ukrainian troops and about eleven thousand international participants to be involved therein (President of Ukraine, 2021m). In addition, previous experience is also analyzed in scientific and research projects related to Ukraine's security and defense sector development. Research institutions have been established and operate under all agencies of the national security and defense sector of Ukraine. In addition, the Ukraine-NATO Platform for identifying lessons learned from the hybrid war in Ukraine has been established to study best practices relating to countering the hybrid warfare in Ukraine.

The lessons learned from past exercises and international cooperation, as well as past events, are used during preparation of strategic and program documents, such as National Security Strategy, Annual National Program under the auspice of the Ukraine-NATO Commission, as well as other planning documents in the spheres of national security and defense.

Important conclusions to determine the national resilience ensuring ways and mechanisms can also be drawn from research into historical experiences. It should be noted, that a lot of attention was paid to the issues of civil defense and resilient functioning of the national economy during the wartime in the USSR. Many mechanisms of civil defense and preparedness of the state for emergencies and war-time were developed and implemented. Thus, regarding the resilience of the national economy Resolutions of the Central Committee of the Communist Party of Ukraine and Council of Ministers of the SSR of Ukraine, dated May 22, 1979, No 267-0011, and the Central Committee of the Communist Party of the Soviet Union [CC CPSU] and the Council of Ministers of the USSR, dated March 30, 1979, No 312-109, were approved. Analysis of general requirements for the enhancement of national economy resilience during war-time approved by the subject Resolution of the CC CPSU and the Council of Ministers of the USSR gives reason to state that these requirements imply numerous principles and approaches that are relevant at the present time. This includes a comprehensive approach to the civil defense measures development; promotion of necessary knowledge and skills, including moral and psychological training of the public, exercises, and trainings; ensuring preparedness of civil defense forces, centralized and local alert systems, and protective facilities (shelters); establishment of necessary reserves; guaranteed continuity of life-sustaining processes and functions (including supply of food, drinking water, essential life necessities, healthcare, utility, and other services); establishing and maintaining continuous information provision to the public.

In addition, the subject documents of the Soviet period focused significantly on security issues during planning of settlements, preparing plans for the potential evacuation of strategic economic facilities and temporary displacement of population, plans of sustainable operation of industries during the war-time, plans of rapid national economy recovery and back-up sets of technical documentation. The main areas of continuous governance were determined, including transitioning from centralized to decentralized administration, generation of pools of personnel, cooperation between sectoral, territorial, and military governance bodies, joint use of control centers, ways of information collection, processing, and sharing. They also envisaged general governance paradigms to be developed for industries as an element of ensuring preparedness for war-time conditions. These approved general requirements and objectives were determined according to different levels of governance: national, local, and sectoral.

After the collapse of the USSR, the young independent nations, including Ukraine, faced many complex issues in the sphere of state building and economic development. With the budget deficit and scarce resources in early 1990-s in Ukraine, a significant part of the mechanisms in the USSR's civil defense system was brought to a standstill.

In general, Ukraine presently lacks a national platform that might be joined, in addition to representatives of public authorities, by representatives from scientific institutions, NGOs, and individual experts to share lessons learned and elaborate on joint solutions in the area of national security and resilience.

The above mentioned summary of systemic problems with national resilience ensuring in Ukraine at legislative, institutional, organizational, and methodological levels will be further analyzed in this monograph in detail. However, based on the above, it can be asserted that existing pending problems at all phases of the national resilience ensuring cycle prove that Ukraine has not met either the resilient criteria of state of the state (reliability, redundancy, adaptability, absorption), or the resilient criteria of functioning of the state (preparedness, efficiency, response, recovery).

Another group of problems asserts that Ukraine has not reached the key resilience criteria related to the state and functioning of society. Thus, despite the outburst of public self-organization and active engagement in response to Russia's aggression against Ukraine, the prevailing notable political absenteeism in society that can be observed in the world according to Joseph (2013), applies to Ukraine as well. However, unlike in developed democracies, the lack of trust in the government and political institutions and disappointment of the public, as well as the low level of political culture in the society, should be referred to as the root causes of this phenomenon in Ukraine.

According to the nationwide poll conducted by the Ilko Kucheriv Democratic Initiatives Foundation [DIF] jointly with the Razumkov Center sociological service on December 15-19, 2017, only 7 % of respondents note that they engage in public activity, while 87% say they take no part in public activity;

over 85 % of respondents have no membership in any public associations; and only about 12 % of respondents engaged in volunteer activities in 2017. In general, according to experts, in 2017 the level of citizen engagement in charity activities was much higher than before the Revolution of Dignity 2014 (DIF, 2018).

According to another nationwide survey, conducted by the Pact organization within the framework of the "Enhance Non-Governmental Actors and Grassroots Engagement" [ENGAGE] activity and funded by the US Agency for International Development [USAID], only 7 % of Ukrainians were actively engaged in their community life, while the other 22 % only occasionally took part in meetings and other events. However, 4 % of citizens actively engaged in civic society organizations, and the other 15 % said they rarely engaged in such activities. The highest level of engagement was observed in residential building, street or neighborhood committees (10%), and involvement in peaceful assemblies (8%) (USAID/ENGAGE, 2018).

The results of another regular round of all-Ukrainian survey concerning civic engagement conducted by the ENGAGE Program in the winter of 2021, showed a still rather low level of Ukraine's citizen engagement in active civic work: only 6.8 % of respondents noted their involvement in peaceful assemblies, while 8 % took part in the establishment or work of residential building, street or neighborhood committees. Another 8.1 % reported on infrastructure issues in person, on the phone, or online. Only 4 % of respondents noted their active engagement in non-governmental organizations' efforts during the past year and 13% stated that they engaged in such events occasionally. Ukrainians were readily involved in their community life, as was noted by one-third (33%) of respondents. Only 7.4 % of respondents attend meetings and other public events of their building, street or neighborhood on a regular basis, while two thirds mentioned they either had no time (33.3 %), or were not interested (31.7 %) in such activities (USAID/ENGAGE, 2021).

The survey regarding opinion concerning the situation in the country, trust in civic institutions and in politicians, and citizen voting inclinations, conducted by the Razumkov Center sociological service in March 2021, demonstrated the following results: among state and civic institutions, the distrust most frequently applies to the government apparatus (functionaries) (80 %), courts (judicial system in general) (79 %), the Verkhovna Rada of Ukraine (77.5 %), the Government of Ukraine (76 %), the High Anti-Corruption Court of Ukraine (73 %), political parties (71 %), Prosecutor offices (71 %), commercial banks (70 %), the National Anti-Corruption Bureau of Ukraine [NABU] (70 %), the Supreme Court (69 %), the Constitutional Court of Ukraine (69 %), the Specialized Anti-Corruption Prosecutor Office of Ukraine [SACPO] (68 %), Ukraine's National Agency on Corruption Prevention [NACP] (68 %), local courts (66%), the President of Ukraine (61.5 %), National Bank of Ukraine (60 %). Most frequently expressed is trust in the Armed Forces of Ukraine (70 % of respondents trust them), volunteer civil organizations (65 %), the Church (64 %), State Service for Emergencies (63 %), State Border Guard Service (60 %), National Guard of Ukraine (56 %), respondent's city (town, village) mayor (56 %), volunteer battalions (55 %), the non-governmental organizations (53 %), the respondent's city (town, village) of residence council (51 %) (Razumkov Center, 2021).

A similar survey, conducted by the Razumkov Center sociological service in June 2018 asserted that among state and civic institutions, the most trust was in volunteer civil organizations (trusted by 65.2 % of respondents), the Church (61.1 %), the Armed Forces of Ukraine (57.2 %), volunteer battalions (50 %), the State Service for Emergencies (51.1 %), the State Border Guard Service (50.7 %), the National Guard of Ukraine (48.6 %), non-governmental organizations (43.4 %). At the statistically significant level, the number of respondents having trust in these institutions exceeded those, who had no trust in them. At the same time, 13.8 % of respondents did, and 80.6 % did not trust the President of Ukraine, 13.7 and 80.7%, accordingly, had or had no trust in the Government, 10.3 and 85.6%, accordingly, in the Verkhovna Rada of Ukraine, 14.1 and 76.2%, accordingly, in the National Bank of Ukraine, 10.6 and 75.2%, accordingly, in the Supreme Court. Trust in the government apparatus (functionaries) was expressed by 8.6% of respondents, and distrust by 85.3 % (Razumkov Center, 2018).

The Razumkov Center experts determined the following specifics of Ukrainian citizens' political culture: the types of political culture involving inherent distrust in policy and political institutions and low interest in politics (61%) (Razumkov Center, 2017). In Europe, similar indicators pertain to Latvia, Bulgaria, and Hungary. Only 8% of Ukrainian citizens can be referred to as positively oriented types of political culture. Note that the level of civic culture that is characterized by high interest in politics and trust in political institutions in Ukraine is one of the lowest in Europe (3.9%), and is far behind the rates in developed democracies, such as Denmark (69.2%), Switzerland (54.3%) and the Netherlands (53 %) (Razumkov Center, 2017).

According to Razumkov Center experts, almost half of Ukrainian citizens recognize no political forces, to which power can be entrusted, or political leaders, who could govern effectively. The majority of citizens believe democracy to be the best type of social system for the state. Only one third of citizens believe their personal involvement is necessary to change the situation in Ukraine for the better. The overwhelming majority of citizens are not involved in active civic processes and have resorted to no forms of communicating their opinions and interests to the state authorities. According to the Razumkov Center expert opinion, political culture in Ukraine can be described as inconsistent, and also, as a combination of aspiration toward personal freedom, demand for leaders that would be accountable to the public, and there is also understanding of the significance of certain institutionalized norms (Razumkov Center, 2017).

It should also be noted, that contemporary Ukraine has no strong traditions of local self-government, although there is a large potential and demand of the population for playing a bigger role in nation building processes. Successful completion of decentralization and public administration reforms is important for building resilience of local communities and regions.

In addition, experts draw attention to an inadequate level of safety culture in Ukraine, both at society level, and the level of organizations and individuals (Hlushak, 2019; Skaletskyi et al., 2012). The lack of appropriate knowledge and behavioral skills regarding action in crises reduces the general level of preparedness of the state and society to respond to threats. In general, the issues of safety culture in Ukraine are known in the context of nuclear energy functionality. However, the notion of a safety culture in society as a specific set of shared values and practices, that can secure the population, enterprises, and organizations, as well as minimize negative effects of threats and crises, is quite common in the world (Center for the Protection of National Infrastructure, 2021; UK National Cyber Security Center, n.d.). A part of such a culture entails active cooperation between the public and law enforcement authorities within the framework of various cooperation programs. As has been noted already, such practices are common in the US, Israel, the UK, and other countries.

In general, the above shows that Ukrainian society has not yet reached the resilience criteria of state (including cohesion and unity, strong ties between various civic groups, involvement of the population in economic, political, and other civic activity, confidence in the government), or the resilient criteria of functioning (regarding effective community governance, understanding by the population of the nature and character of threats and the procedure to follow in case of their occurrence, preparedness to respond to threats, control over the situation prior to, during, and after the crisis, establishment of joint capabilities to counter threats, crises).

Considering the theoretical conclusions in Chapters 1 and 2 of the monograph regarding the “weaknesses” in ensuring resilience and vulnerabilities, which define the general level of complex systems resilience, it can be assumed that the current level of resilience of the state and society in Ukraine is insufficient.

Thus, systemic national resilience ensuring mechanisms, which should improve adaptability of security policy and management of key functions of the state and society in uncertain and rapidly changing security environment, and root out conditions creating vulnerabilities in the state and society, have not been established in Ukraine up to date. However, there is a vigorous state and society resilience potential that needs to be strengthened and developed.

Based on the above, it can be stated that the *need to create a national resilience ensuring system in Ukraine is fully justified*. In view of limited state resources and existing systems and mechanisms for ensuring national security, public administration, and crisis management, a national resilience ensuring system should be built *taking into account existing linkages through the implementation of resilience principles across various governance areas*. Considering similarities between national security and national resilience ensuring actors and objects, organizationally the relevant system can be established as a sub-system within the national security ensuring system, or as a related to it system. In the future, it would be expedient to think about potential upgrading and integration of these systems into *a comprehensive national security and resilience ensuring system*.

5.3. Systemic Problems with Providing National Resilience in Ukraine in a Changing and Uncertain Security Environment

5.3.1. The Problems of Setting National Resilience Ensuring Goals and Objectives in Strategic Documents of Ukraine

In the context of determining political vectors, goals, and objectives in the sphere of national security and resilience, it is important to develop, adopt and implement strategic and program documents of the state, in particular the National Security Strategy. Such documents highlight the system of official views on the role and place of the state in the modern world, its national values, interests, and goals, as well as capabilities, tools, and ways to prevent and address external and internal threats. The relevant laws set out principles and rules of organization and functioning of the national resilience ensuring system, and clauses in subject strategic and program documents can specify the directions of its development or reform.

Presently, the main regulatory act, according to which planning in the sphere of national security and defense is carried out, including drafting of appropriate strategic documents, is the Law of Ukraine "On the National Security Strategy of Ukraine" (hereinafter – Law) (Law of Ukraine, 2018).

According to par. 15, Part 1, Article 1 of the Law, planning in the field of national security is a function of public administration to determine priorities, tasks, and measures to ensure the national security of Ukraine, balanced development of components of the security and defense sector based on security situation assessment and taking into account financial and economic capabilities of the state.

The goal of planning in the areas of national security and defense is to ensure the implementation of government policy in these areas through development of strategies, concepts, programs, and plans for security and defense sector components development, resource management, and effective allocation. Planning in the areas of national security and defense shall correspond to the following principles: 1) adherence to the national legislation and international commitments of Ukraine; 2) democratic civil control of the national security and defense sector, free access to information concerning the public policy, strategic documents, goals, priorities, and objectives of planning, transparent and accountable use of resources; 3) holistic, consistent and systemic approaches to planning in national security and defense sector, consideration of priorities and limits, as set forth in the government programs, plans and forecasting documents; 4) timeliness and compliance with decisions concerning protection of national interests of Ukraine – due to the Parts 1 and 2, Article 25 of the Law.

The National Security Strategy of Ukraine is a basis for all other documents with regard to planning in the areas of national security and defense. The implementation of the National Security Strategy of Ukraine is based on the national defense, security, economic and intellectual potential using the mechanisms of public-private partnerships, as well as international counseling, financial and technical assistance (Part Three, Article 26 of the Law).

The Law sets out requirements for the procedure of development, purposefulness, and structure of the National Security Strategy of Ukraine, and subsequent specific strategic planning documents, such as the Military Security Strategy of Ukraine, Cybersecurity Strategy of Ukraine, Civil Security and Civil Protection Strategy of Ukraine, Strategy for the Development of the Defense Industrial Complex of Ukraine, as well as the National Intelligence Program. According to the Law, the National Security Strategy of Ukraine outlines the following:

1) the priorities of national interests of Ukraine and ensuring national security, the goals and main areas of public policy in national security;

2) the current and projected threats to the national security and national interests of Ukraine with consideration of geopolitical and domestic conditions;

3) key areas of geopolitical activities of the state to ensure its national interests and security;

4) the directions and objectives of security and defense sector reform and development;

5) resources required for implementation of the Strategy.

Before 2018, the legal framework for strategic planning in the sphere of national security of Ukraine was provided by the Law of Ukraine “On the Foundations of the National Security of Ukraine” (Law of Ukraine, 2003b), making the National Security Strategy of Ukraine, Cybersecurity Strategy of Ukraine and Military Doctrine of Ukraine the mandatory documents and the basis for the development of programs in terms of the components of state national security policy. The subject Law did not set out a procedure for the development of such documents, their directions and structure, but in practice, they identified threats to national security, priority areas, and objectives for the security policy of the state. Strategic planning process in the relevant area was regulated by the Law of Ukraine “On the Defense Planning” (Law of Ukraine, 2005).

The first National Security Strategy of Ukraine was adopted in 2007 (President of Ukraine, 2007). The document outlined a rather broad spectrum of threats to national security, many of which remain relevant to date. These concerns, in particular, the failure of the national security sector of Ukraine to meet the needs of society, insufficient national cohesion and consolidation in society, negative external influences on the information environment, terrorism. Meanwhile, the objectives of state policy in national security were defined largely declaratively, which did not contribute to the achievement of certain goals to overcome or minimize the effects of threats.

The President of Ukraine approved the subsequent National Security Strategy in 2012 (President of Ukraine, 2012). It reflected the changes that had taken place in Ukraine’s security environment at the time and set out important objectives in the sphere of protection of interests of an individual, society, and the state. Thus, it set forth the requirement to implement judicial and administrative reform; counter corruption; reform security and defense sector as an integral system, strengthen its functional capability; improve public spending effectiveness; ensure effective control of monopolies; diversify energy sources, improve their effectiveness; address disproportion in social and humanitarian spheres; creating safe living conditions for the population, and other important measures. However, no significant progress in the implementation of this Strategy was made, as the objectives outlined in this document remained unaccomplished for the most part.

Although the overwhelming majority of threats and priorities of national security policy were applicable as of 2014, the situation inside and around Ukraine has changed radically as Russia’s large-scale aggression against Ukraine began. The response had to be immediate to protect the national sovereignty and territorial integrity and save the lives of Ukrainian citizens. Since Ukraine has not been and is not currently a member of international military or political alliances, it had to rely solely on its own capacity, and this required a corresponding redistribution of state resources and a review of priorities in the field of national security and defense.

In view of major changes in the security environment, the issue on the agenda was an update of the National Security Strategy of Ukraine. In addition, according to the Strategy 2012, Ukraine had to adhere to a non-block status, and Russia was defined as a strategic partner, which in 2014 corresponded to neither reality nor its national interests.

In 2015, a new version of the National Security Strategy of Ukraine was approved by the President of Ukraine (2015b). This document clearly stated that the greatest threat to Ukraine at the moment was the aggressive actions of Russia, which are carried out to deplete the Ukrainian economy and undermine socio-political stability in order to destroy the Ukrainian state and seize its territory. The key areas of the state policy in the national security of Ukraine were identified as restoration of territorial integrity of Ukraine; establishment of effective security and defense sector; enhancement of defense capacity of the state; reform and development of intelligence, counter-intelligence, and law-enforcement agencies; public administration system reform; ensuring new quality of anti-corruption policy; providing integration with the EU and special partnership with NATO. In addition, a range of essential measures was identified in key areas of national security: foreign policy, economic, energy, information, cyber, environmental, and critical infrastructure protection.

The 2015 National Security Strategy sets out rather clear objectives of public policy in national security versus previous versions of this document. In addition, those objectives correspond to other national policies, such as Coalition Agreement and Sustainable Development Strategy “Ukraine – 2020.” However, none of these three documents was fully implemented.

Specifically, no tangible progress was made with the following objectives of the National Security Strategy of Ukraine 2015 implementation: effective coordination and operation of integrated system of situational centers at authorized agencies and within the security and defense sector; improvement of democratic civil control over security and defense sector, strengthening of parliamentary control in this sphere; development of military patriotic education system, introduction of military training and civil protection curricula at secondary education, vocational/technical schools, and higher education; reform of the Security Service of Ukraine; cleaning state power of corrupt and incompetent personnel, politically motivated decision-making, preventing the predominance of personal, corporate, regional interests over national ones; public service system reform; overcoming poverty and excessive property stratification in society; ensure deoligarchization and demonopolization of economy, protection of economic competition, taxation simplification and optimization; effective application of special economic and other restrictive measures (sanctions) mechanism; enhancement of national economy resilience against negative external influences, diversification of external markets, trade and financial routs; comprehensive improvement of legal framework on critical infrastructure protection, establishment of a system of its security public management; establishment of effective environment monitoring system; ensuring resource conservation and sustainable use of nature.

The Sustainable Development Strategy “Ukraine-2020,” approved by the President of Ukraine (2015c), set out the implementation of 62 reforms and programs to implement European standards of living in Ukraine and gaining by Ukraine of leading positions in the world. However, only few determined objectives were accomplished (Annex 1).

Thus, former versions of the National Security Strategy of Ukraine, approved in 2007, 2012, and 2015, included description of relevant at the time external and internal threats and global security environment development trends, and state policy priorities in national security. However, the level of fulfillment of these documents remained rather low, while some objectives (specifically concerning fight against corruption, reform of the security and defense sector and public administration system) were repeated practically in each of them.

In addition to lack of political will for changes, the lack of clear plans for Strategy implementation across different national security areas (except defense area and later the cybersecurity area) contributed to the situation significantly. Control of strategic documents fulfillment was a formality, no reporting procedures or outcomes evaluation indicators or criteria were established, or their adherence to the goals analyzed.

The Law of Ukraine "On National Security of Ukraine" (Law of Ukraine, 2018), adopted in 2018, created a legal framework for building a new quality national security ensuring system to meet the up-to-date requirements. Skilled Ukrainian and international experts, government and civil society representatives were involved in drafting of the subject law. It is important that NATO and EU principles and standards in ensuring national security were considered in the draft law.

This basic law determines the legal framework of the relevant sphere of social relations, and its provisions were detailed and refined in other laws and by-laws. Even though the "national resilience" definition is not mentioned in the Law, it allows for the incorporation of appropriate principles into new versions of the National Security Strategy of Ukraine.

The current National Security Strategy of Ukraine "Security of an individual – security of the country" (hereinafter – the Strategy) was developed taking into account the up-to-date tendencies in the development of guidelines for strategic planning and management in the field of security, and also, lessons learned by Ukraine from countering hybrid aggression. In this document versus the previous versions, a much bigger focus is placed on human rights and interests protection (President of Ukraine, 2020b).

The key principles underpinning the Strategy include deterrence, resilience and cooperation. The appropriate definitions are provided in paragraph 4 of the document:

deterrence is the development of defense and security capabilities to prevent armed aggression against Ukraine;

resilience is the ability of society and the state to adapt rapidly to the changing security environment and maintain sustainable functioning, including by minimizing external and internal vulnerabilities;

cooperation is the development of strategic relations with key foreign partners, primarily with the European Union and NATO and their Member Nations, the United States of America, and pragmatic cooperation with other states and international organizations based on the national interests of Ukraine (President of Ukraine, 2020b).

In the former versions of the National Security Strategy of Ukraine, resilience was mentioned only once in the 2015 document with regard to improving the national economy resilience against negative external impacts. This notion was previously used in legal documents of Ukraine primarily in economic spheres (within the context of resilient economic development, resilience of banks, banking system, and insurers), medicine, and biosecurity.

Par. 47 of the current Strategy for the first time ever sets out the necessity to build up a national resilience ensuring system and the requirements thereto. However, the insufficient and inconsistent regulations with regard to ensuring national resilience, including the lack of legislative definition of the term "national resilience," the organizational model, principles, and mechanisms, powers, tasks, and responsibilities of state and local authorities, enterprises and organizations, and civil society actors' rights and obligations – all of these implied the risks of failing the Strategy objective and required definition of the *conceptual framework of national resilience ensuring in Ukraine*.

These problems were partially addressed by the National Security and Defense Council of Ukraine's Decision, enacted by the President of Ukraine (2021g), which approved the Concept of Support of the National Resilience System. At the same time, the efforts concerning Ukrainian legislation improvement to accomplish the tasks, as set out in the subject Concept, and to address other problem areas in the sphere of ensuring national resilience, continue.

Currently, a number of Ukrainian ministries and agencies implement specific sectoral measures to enhance resilience in their areas of responsibility. Thus, the National Police of Ukraine has implemented a situational management model, while police divisions and units plan security measures based on the single "threat model" document, which is developed for each police body taking into account local conditions; the Approximate action algorithm has been developed; operational plans are developed to improve resilience of police bodies under special conditions. The State Emergency Service of Ukraine has improved the processes of fire, man-made emergency, and natural disaster risk management, their monitoring and forecasting, and information sharing with other states has been streamlined. To promote the necessary knowledge and skills, the Ministry of Interior of Ukraine jointly with the State Emergency Service, National Police of Ukraine, State Border Guard Administration of Ukraine, and National Guard of Ukraine elaborated on the Draft Concept of the national educational system in the sphere of critical infrastructure protection. The National Police of Ukraine has improved the response system, including the "102" integrated contact centers receiving information concerning emergencies, and a dispatch operator service providing centralized control of police patrols at region level; a new mobile application operating all over Ukraine has been implemented. To raise public awareness concerning emergency management, location of shelters and healthcare facilities, the State Emergency Service established a provisional approach to informing the public via existing network of the "101" dispatch services and counseling centers at territorial branches of the Service, and the mobile application testing is going on.

However, it does not seem possible to evaluate the effectiveness of scattered sectoral resilience strengthening measures due to the lack of uniform conceptual approaches and appropriate criteria.

In Quarter IV, 2020, Ukraine launched a major process of strategic planning documents development in the spheres of national security based on provisions of the National Security Strategy of Ukraine (Reznikova, 2020e). These concern the

Human Development Strategy, Military Security Strategy of Ukraine, Civil Security and Civil Protection Strategy of Ukraine, Strategy for the Development of the Defense Industrial Complex of Ukraine, Economic Security Strategy, Energy Security Strategy, Environmental Security and Adaptation to Climate Change Strategy, Biosafety and Biosecurity Strategy, Information Security Strategy, Cybersecurity Strategy, Foreign Policy Strategy of Ukraine, Strategy for Security of the State, Integrated Border Management Strategy, Food Security Strategy, and National Intelligence Strategy.

Sectoral security strategies are level two planning documents. They are integrated decision systems focusing on the achievement of clearly outlined socially significant goals and outcomes in the future (for the period of five plus years). They should take into account, but not be limited to, the current and projected threats, trends in security environment, and national interest priorities, as set out in the National Security Strategy (level one document). Sectoral strategies are detailed in action plans for their implementation.

However, at the time of strategic planning documents development in the areas of national security, the conceptual framework of national security and resilience ensuring system in Ukraine was incoherent, thus allowing for no clear formulation of appropriate integrated objectives in the sectoral security strategies. No coherence has been observed between the government documents setting out objectives in the sphere of ensuring national resilience and sustainable development in Ukraine (Reznikova, 2019a). Strategic planning process in the field of national security is made more difficult by the lack of consolidated requirements to methodology for preparation of certain documents and organization of the process, including inter-agency cooperation.

The organization and maintenance of document preparation in the areas of national security have uncovered a range of problems of methodological and organizational nature. Thus, some ministries and agencies, as developers of planning documents, paid inadequate attention to analysis of security situation in relevant areas, risk assessment and projections, identification of threats and detection of vulnerabilities. The focus of some state authorities on addressing current problems is not helpful in creating a vision for the future.

Inefficient control of accomplishment of objectives, as set out in the National Security Strategy, increases the risk of failing to implement this document in full. Thus, of fifteen documents regarding planning in the areas of national security and defense, which should have been developed and approved within six months (before 14 March 2021) due to the National Security of Ukraine Strategy 2020,[25] only the 2021–2025 National Intelligence Program was approved and the Strategy for Integrated Border Management until 2025 was amended on time, and only six documents were approved before September 1, 2021: Military Security Strategy of Ukraine, Human Development Strategy, Economic Security Strategy until 2025, Strategy for the Development of the Defense Industrial Complex of Ukraine, Cybersecurity Strategy of Ukraine, and Foreign Policy Strategy of Ukraine[26] (Cabinet of Ministers of Ukraine, 2019b; President of Ukraine, 2020b, 2021b, 2021c, 2021d, 2021f, 2021i, 2021j).

The issue of full and effective implementation of the National Security Strategy of Ukraine is still relevant. To achieve the ambitious goals, as set out in the current document, so that the appropriate objectives do not remain yet another declaration.

Based on the results of the analysis, it can be concluded that organizational, institutional, and legal ambiguity considerably hurdles the processes of building national resilience in Ukraine. In addition, inadequate Ukrainian legislation in the sphere of strategic planning contains the risks of inconsistency and failure to fulfill the relevant documents to the full extent in the context of implementing measures on strengthening national resilience.

[25] According to President of Ukraine (2020b).

[26] As of 31 December 2021, in total 12 of 15 documents regarding planning in the areas of national security and defense that were required to be developed by the National Security Strategy of Ukraine, were duly approved.

5.3.2. Terminological Inconsistency in the Sphere of National Resilience in Ukraine

A number of strategic and program documents of the state (including the National Security Strategy of Ukraine 2020, the Annual National Program under the auspices of the Ukraine-NATO Commission for 2020 (hereinafter – ANP-2020), the Annual National Program under the auspice of Ukraine-NATO Commission for 2021 (hereinafter – ANP-2021), the State Regional Development Strategy during 2021–2027) set out national resilience system building priorities (President of Ukraine, 2020a, 2020b, 2021a; Cabinet of Ministers of Ukraine, 2020a). However, considering the lack of legislation in the field of national resilience in Ukraine, there is a range of problems concerning the use of key terms in the relevant sphere, which complicates the accomplishment of objectives that have been set.

The key definitions in the field of national resilience were provided only recently in the Concept of Support of the National Resilience System, approved the by President of Ukraine (2021g). However, changes to the legislation in order to streamline the use of terminology in the relevant field have not yet been introduced.

Systemic analysis of Ukraine's legislation, including the laws of Ukraine "On National Security of Ukraine," "On Defense of Ukraine," "On Armed Forces of Ukraine," "On Combating Terrorism," "On Security Service of Ukraine," and also National Security Strategy of Ukraine 2020, ANP-2020, ANP-2021, State Regional Development Strategy 2021–2027, allowed for several conclusions to be made (Reznikova & Voytovskyi, 2021).

Firstly, prior to the adoption of the Concept of Support of the National Resilience System, the Ukrainian legislation included no commonly used language in the sphere of national security definitions, such as of "national resilience," "national resilience system," "capability," "preparedness," or "vulnerability," thus causing inconsistencies in the setting and accomplishment of appropriate objectives.

Secondly, a number of regulatory acts of Ukraine mention or provide certain definitions associated with resilience, though specific in nature as they refer to different areas (branches), thus requiring detailing on their specific applicability.

In particular, the terms relating to resilience in specific areas are used in the following legislative and regulatory acts of Ukraine: Concepts of establishing critical infrastructure protection systems (Cabinet of Ministers of Ukraine, 2017a) ("critical infrastructure resilience," "resilience of communities"); Decree of the President of Ukraine "On the Sustained Development Goals of Ukraine until 2030" (President of Ukraine, 2019e) ("ecological resilience of towns"); ANP-2020 ("financial resilience," "social resilience," "resilience of infrastructure," "interference resilience," "resilient network," "resilient community," "resilient communications," "resilient management"); ANP-2021 ("social resilience," "financial resilience," "national resilience system," "critical infrastructure resilience"); State Regional Development Strategy 2021–2027 ("resilience to disasters," "resilient growth of standards of living," "resilience to water temperature changes").

Thirdly, a systems approach to building national resilience has been used only in a few regulatory acts of Ukraine, such as the National Security Strategy of Ukraine 2020, ANP-2020, and ANP-2021.

It should be noted, that the word combination "national resilience system" is used in this and other regulatory acts of Ukraine in the meaning of "national resilience ensuring system," which is an organizational and regulatory mechanism streamlining activities of the system's actors in line with the specified model and national interests.

Fourthly, in several regulatory acts of Ukraine such terms as "survivability" and "reliability" are present; their meanings are close to the term "resilience." They usually define certain features of technical systems and their ability to stand up to specific threats.

For instance, the notion of "survivability" is used in the Legislation of Ukraine (2003, 2004, 2017b, 2018a). In the laws of Ukraine "On Defense of

Ukraine," "On Combating Terrorism" (Law of Ukraine, 1992, 2003a), the National Security Strategy of Ukraine 2020, ANP-2020, ANP-2021, this term is used in other word combinations along with the term "reliability."

Fifthly, in various regulatory documents of Ukraine the non-systemic use of other terms associated with national resilience, including such definitions as "capabilities," "vulnerabilities," and "preparedness" can be observed.

Specific definitions of "capability" that are used in certain areas may appear, for instance, in the documents by the Cabinet of Ministers of Ukraine (2018, 2019c), President of Ukraine (2019b), Legislation of Ukraine (2018b). All definitions in those and other documents have certain semantic differences. In addition, in the laws of Ukraine "On National Security of Ukraine," "On the Armed Forces of Ukraine" (The Law of Ukraine, 1991, 2018), National Security Service of Ukraine 2020, ANP-2020, ANP-2021, State Regional Development 2021–2027, the term "capability" appears in word combinations that have no clear explanation.

Specific definitions of the term "vulnerability" (including in word combinations) appear, for instance, in the documents by the President of Ukraine (2019a), Legislation of Ukraine (2017a, 2020a). These definitions also have semantic differences in line with specifics of a relevant area. In addition, in the National Security Strategy of Ukraine 2020, ANP-2020, and ANP-2021, the term "vulnerability" is used in word combinations with no proper explanation provided.

Specific definitions of "preparedness" term (including word combinations) are provided for example, in the Legislation of Ukraine (2004, 2011, 2015). In addition, the laws of Ukraine "On Defense of Ukraine, "On National Security of Ukraine," "On the Armed Forces of Ukraine," and also the National Security Strategy of Ukraine 2020, ANP-2020, ANP-2021, and the State Regional Development Strategy during 2021-2027 use the term "preparedness" with no proper explanation provided.

The above mentioned shows that the variety and inconsistency of terms related to ensuring resilience and used in Ukrainian legislation and professional literature do not contribute to a common understanding of the objectives, set by the leadership of the state, and their effective implementation. This raises the issue of harmonizing the terms used in various legal acts with their content, defined in the Concept of Support of the National Resilience System.

5.3.3. Problems in the Sphere of National Resilience Providing Organizational Support

The world experience proves that effective national resilience ensuring systems are rather decentralized, and decisions regarding response are taken at the lowest possible level. At the same time, coordination of efforts, establishment of consistent and clear for all actors rules, standards, and procedures at all phases of the national resilience ensuring cycle are important. This generally takes place at the highest possible levels that each country determines on its own. In the parliamentary democracy this function is usually performed by the government. Many countries introduce universal mechanisms of coordination and cooperation between central and local authorities, which should be approximated to the maximum possible extent both during peacetime and wartime. In addition, one of the key areas in building national resilience is effective cooperation between governmental and non-governmental actors in different areas prior to, during and after the crisis. Thus, appropriate organizational and legal support for such activities in the state is crucial.

An existing distribution of constitutional powers between different branches of power in Ukraine (primarily between the President of Ukraine, the National Security and Defense Council of Ukraine, and the Cabinet of Ministers of Ukraine) is a critical problem in terms of coordination and control in the field of national security and resilience, considering that this complicates the development of consolidated and functional national security and resilience ensuring system managed from a single center. As stated above, the functioning of a few centers at the same level of coordination in parallel increases inconsistencies and the risk of disruption and disequilibrium of the system (Bogdanov, 2003). In addition, the lessons learned from countering the hybrid aggression and the COVID-19 epidemic have revealed gaps in the mechanisms of coordination between various actors in crises, such as central and local authorities, non-governmental institutions, and the public.

According to Ukraine's Constitution, the powers in the sphere of national security and crisis management are distributed between the President of Ukraine, the National Security and Defense Council of Ukraine, and the Cabinet of Ministers of Ukraine (Law of Ukraine, 1996). According to pars. 1, 17, Part 1, Article 106 of the Constitution, the President of Ukraine ensures national security and provides leadership in the spheres of national security and defense of the state. According to the Law of Ukraine "On National Security of Ukraine" (Article 13), the spheres of national security and defense are managed through the realization by the President of Ukraine of the totality of his constitutional powers (Law of Ukraine, 2018).

According to Article 107 of Ukraine's Constitution, the National Security and Defense Council of Ukraine coordinates and controls activities of executive authorities in the sphere of national security and defense (Law of Ukraine, 1996). As such, according to Part 1, Article 14 of the Law of Ukraine "On National Security of Ukraine," the NSDC of Ukraine carries out coordination in the spheres of national security and defense. Thus, Part 2, Article 14 of the Law, provides that in martial law or emergency, and if crises occur, the NSDC of Ukraine shall coordinate activities of executive authorities and review proposals concerning special economic and other restrictions to be applied. During martial law, according to Part 3, Article 14 of the Law, a high strategic panel can be established to take charge of the military leadership for the state's defense. However, coordination of state authorities' activities was not clearly outlined for the NSDC of Ukraine at the phase of threat prevention and ensuring preparedness or post-crisis recovery of full-fledged functionality (Law of Ukraine, 2018).

According to Article 116, Constitution of Ukraine, the Cabinet of Ministers specifically directs and coordinates the work of ministries and other executive authorities and takes measures to ensure defense capacity and national security of Ukraine, public order, and the fight against crime. Article 6, Code of Civil Protection of Ukraine, sets forth that coordination of activities of executive authorities in the sphere of civil protection has to be provided by the National Security and Defense Council of Ukraine and the Cabinet of Ministers of Ukraine within the scope of their powers. To coordinate activities of central and local authorities, enterprises, institutions, and organizations in the areas of ecological safety with regard to natural and technogenic emergencies, protection of population and territories, prevention and response to emergencies, the inter-agency commissions shall be established at different levels. Thus, the Cabinet of Ministers of Ukraine has to establish a State Commission on Technogenic and Environmental Safety and Emergencies. That said, civil protection is defined as the function of the state related to the protection of population, territories, the environment, and property by preventing emergencies of this kind, eliminating their consequences and assisting victims during peacetime and martial law (Law of Ukraine, 2013a).

Therefore, the role of coordination of activities of different state authorities in the areas of national security and civil protection of the population is distributed between the Cabinet of Ministers of Ukraine and the NSDC of Ukraine depending on the situation. No potential involvement of non-governmental agents and the population or coordination of such activities has been clearly defined by Ukrainian legislation (Reznikova, 2020a).

By Decree of the President of Ukraine (2019d), the Commission for Euro-Atlantic Integration of Ukraine was established. Also, this document designated the national coordinators for various issues regarding cooperation between Ukraine and NATO, and the NSDC Ukraine Secretary’s first deputy or one of the deputies was designated as national coordinator in the sphere of building national resilience. However, such an approach seems to be too narrow, as it standardizes just one aspect of coordination with regard to building national resilience at the level of the state, such as international cooperation. Meanwhile, the main problem issues in the sphere of coordination of such activities remain unregulated.

One telling example is the establishment of the National Cybersecurity Coordination Center as a working body of the NSDC of Ukraine, and its mission included coordination and control of security and defense sector actors responsible for ensuring cybersecurity (President of Ukraine, 2016a). An appropriate regulatory document identified a range of objectives in the sphere of cybersecurity and cyber-resilience of critical infrastructure facilities, including analysis of cybersecurity ensuring entities' preparedness to accomplish their mission of countering cyber threats and implementing preventive measures in combating cybercrime, development of the conceptual framework and proposals regarding improvement of the effectiveness of measures to identify and address the factors that generate potential and actual risks in the sphere of cybersecurity, drafting appropriate programs and plans concerning their prevention and mitigation.

The existing situation significantly slows the implementation of such an important principle of national resilience, as a comprehensive approach to the response to all types of threats and hazards, and inclusivity and broad cooperation requiring an integrated system to be established to coordinate efforts of various actors at all phases of the evolving crisis or threat.

As was noted, the effective national security policy formulation and implementation are hurdled significantly by the lack of clearly articulated structure, goals, and objectives of the national security ensuring system, and clear procedure of cooperation between its actors during peacetime and during crises (Reznikova et al., 2015). This and a number of other reasons made it obvious in early 2014 that the security and defense sector of Ukraine, being the most crucial element of the national security ensuring system, had not yet been completed and was not prepared to act as a functional assembly governed by an integrated center.

A number of challenging issues in the organization of the national security ensuring system, crisis management, and public administration in Ukraine hinders the implementation of systemic national resilience ensuring mechanisms. In addition to the lack of clearly distributed responsibilities for different aspects of ensuring national security and crisis management between various branches of government, there are other problems, such as:

- the lack of government authorities responsible for coordination of cooperation between governmental and non-governmental entities in terms of ensuring national resilience at the national and other levels, including in the areas of risk assessment and management, and building appropriate capabilities, generation of necessary reserves, risk analysis, and threat identification, maintenance of national threat register:
- a lack of effective whole-of-government cooperation mechanisms and formats (entities) in the area of ensuring resilience at the national, regional and local levels on a permanent basis;
- a lack of appropriate units or shortage of qualified personnel at existing divisions of government authorities, responsible for ensuring national resilience in different areas;
- underdeveloped public-private partnership in the field of ensuring national security and resilience.

Due to the lack of legislation in Ukraine that would define the mission, roles, and responsibilities of state and local authorities, and other actors in the sphere of national resilience, the response to threats and emergencies, their prevention, ensuring preparedness of the state and society, post-emergency recovery efforts are managed within the framework of basic legislation in the areas of national security and civil protection and subject-matter regulatory acts.

Certain types of threats are responded to within the framework of existing national systems, such as the Unified State Civil Protection System (Cabinet of Ministers of Ukraine, 2014); Integrated state system for the prevention, response, and cessation of terrorist attacks and minimization of their effects (National Counter-Terrorism System) (Cabinet of Ministers of Ukraine, 2016); Emergency

Medical Services System (Law of Ukraine, 2013b); National Cybersecurity System of Ukraine (Law of Ukraine, 2017); Defense Capability Ensuring System of Ukraine (Law of Ukraine, 1992), and other (Annex 2). In addition, the legislation envisages the establishment of the state critical infrastructure protection system (Cabinet of Ministers of Ukraine, 2017a). The organizational and regulatory mechanisms of subject systems encompass the whole territory of the country, while some of these national systems comprise functional and territorial subsystems. Each of them is based on the principles of legitimacy, centralized governance, unity of command, subordination, coordination, maximum possible risk mitigation, and broad cooperation, including with local authorities.

In summary, the key objectives of these systems are to protect:

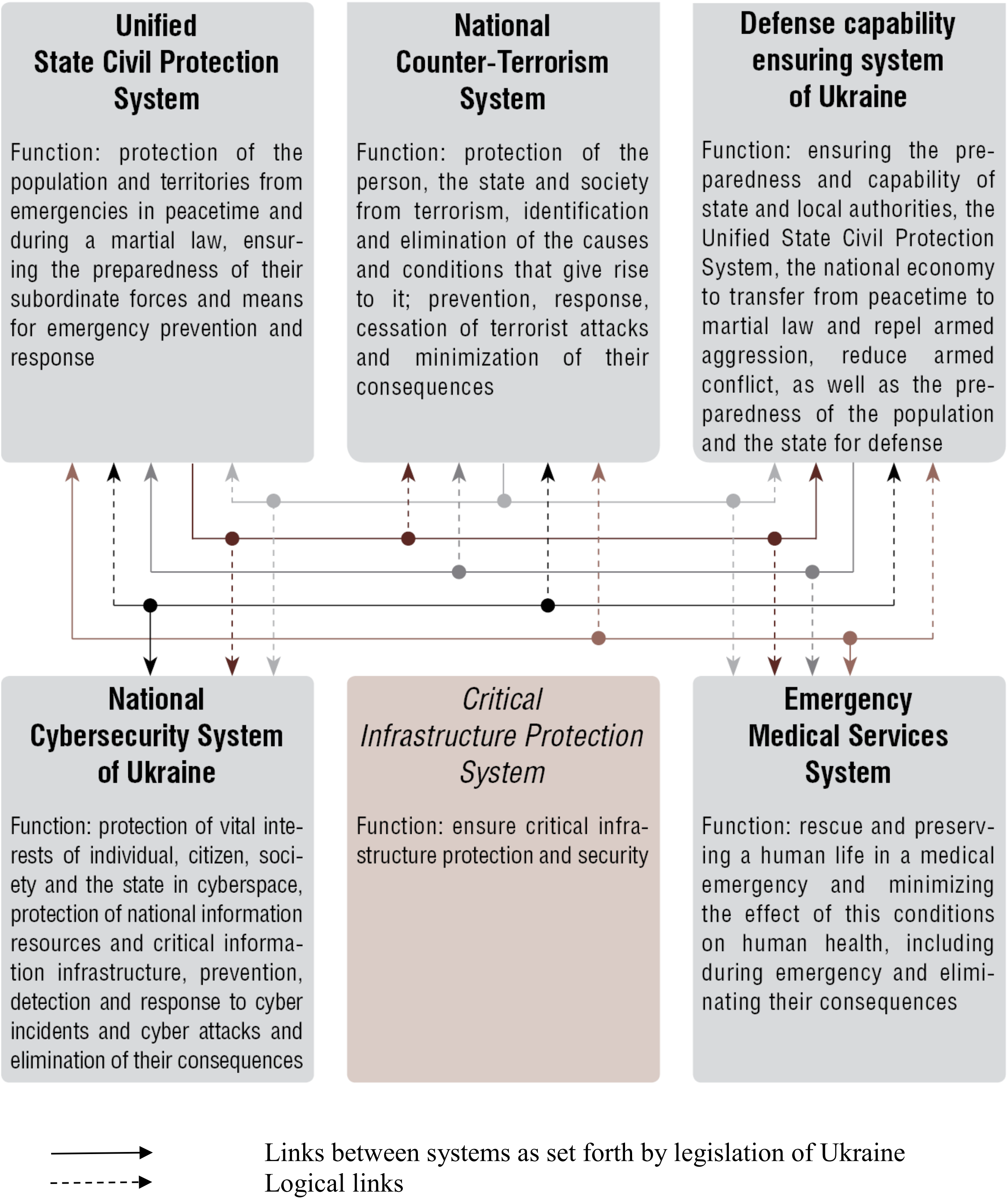
a) the population from natural, man-induced, environmental, biological, chemical, radiological, social, terrorist, military, and other threats and emergencies;

b) the life-sustaining systems of the state and society, including local communities, related to supplies of energy resources, food, drinking water, and also to ensure healthcare and emergency medical services, policing, tele- and radio communications, cybersecurity, transport communications, housing and utility infrastructure:

c) the high-risk facilities located in regions and in the territory of local communities.

A number of challenging issues can be identified based on the analysis of operation and cooperation between the essential national systems providing protection of the state and society from identified threats and emergencies (Reznikova et al., 2021).

The existing *national systems of response to certain threats and emergencies*, (Unified State Civil Protection System; Emergency Medical Services System; National Counter-Terrorism System; National Cybersecurity System of Ukraine; Defense Capability Ensuring System of Ukraine), that are functioning at national, regional, and local levels, include certain partially overlapping inter-agency cooperation formats. Meanwhile, *legislation has no clear definition of a mechanism to coordinate the functioning of subject systems and links between existing inter-agency cooperation formats in the field of threat, crisis, and emergency prevention and response, and further recovery efforts. Numerous existing coordinating authorities and inter-agency groups operate in a narrow field of disparate areas of responsibility.* Fig. 4.1 presents the linkages between different national systems due to the Ukrainian legislation. However, as can be seen in the diagram, direct linkages (marked in continuous lines) only exist between a few systems, while merely informal (logical) linkages (marked in dash lines) exist between others.



Unified State Civil Protection System

Function: protection of the population and territories from emergencies in peacetime and during a martial law, ensuring the preparedness of their subordinate forces and means for emergency prevention and response

National Counter-Terrorism System

Function: protection of the person, the state and society from terrorism, identification and elimination of the causes and conditions that give rise to it; prevention, response, cessation of terrorist attacks and minimization of their consequences

Defense capability ensuring system of Ukraine

Function: ensuring the preparedness and capability of state and local authorities, the Unified State Civil Protection System, the national economy to transfer from peacetime to martial law and repel armed aggression, reduce armed conflict, as well as the preparedness of the population and the state for defense

National Cybersecurity System of Ukraine

Function: protection of vital interests of individual, citizen, society and the state in cyberspace, protection of national information resources and critical information infrastructure, prevention, detection and response to cyber incidents and cyber attacks and elimination of their consequences

Critical Infrastructure Protection System

Function: ensure critical infrastructure protection and security

Emergency Medical Services System

Function: rescue and preserving a human life in a medical emergency and minimizing the effect of this conditions on human health, including during emergency and eliminating their consequences

Links between systems as set forth by legislation of Ukraine

Logical links

Fig. 4.1. **Linkages between national systems in the sphere of threat and emergency response in Ukraine**

Source: Reznikova et al., 2021.

Taking into account systemic analysis of paragraphs 24, 25, Article 2, Civil Protection Code of Ukraine (Law of Ukraine, 2013a) and sub-paragraphs 2, 3, Article 2, Law of Ukraine “On Combating Terrorism” (Law of Ukraine, 2003a), it can be assumed that an emergency may be caused, inter alia, by a terrorist attack.

The role of ensuring preparedness and response to such a situation is assigned to the Unified State Civil Protection System and the National Counter-Terrorism System, and the appropriate powers are vested in regional and local commissions on technogenic and environmental safety and emergencies, and the Anti-Terrorist Center coordination groups at regional offices of the Security Service of Ukraine. In addition, an emergency caused by a terrorist attack poses a serious threat to human lives or health. Therefore, the actors of the Emergency Medical Services System will also be involved in the relevant relief measures. At the same time, the procedures for interaction in complex crises with cascading effects as well as the term “crisis” have not been provided by the legislation of Ukraine.

A comprehensive information-sharing process regarding all potential threats and emergencies has not been established. The relevant processes are in place in certain areas (cybersecurity, counter-terrorism), but they have no system character. Situation and crisis centers at different ministries and agencies are not currently integrated into a single network. This hinders generation of data catalogs and databases required for analysis, projections, and planning in the field of national security.

The lack of effective and consistent inter-agency cooperation in the sphere of national security and resilience hinders the implementation of a comprehensive approach to ensuring preparedness to respond to threats of different origins and major crises.

The legal regulation of preparedness and response to certain threats and emergencies ensuring processes has been scattered all over different legislative and regulatory acts of Ukraine. The definitions, organizational mechanisms, and methodological approaches found in these documents are often not harmonized.

The threat and emergency response during peacetime (without introduction of a legal regime of emergency state, including in a certain territory) mechanisms and protocols are specified in different regulatory acts depending on the area of activity. Such a narrow departmental or sectoral approach creates difficulties due to inconsistency of some legal norms and rules, particularly where prevention or response to threats with cascading effects or of hybrid type are concerned. This, in particular, was proven, when a set of the counter-COVID-19 measures was generated and implemented at regional and local levels, and their implementation was to be ensured by different actors (Kovalivska, 2020).

In addition, there are discrepancies in Ukrainian laws with regard to determining the powers of certain state authorities, the functioning of particular national systems. Thus, the Law of Ukraine "On Combating Terrorism" (Law of Ukraine, 2003a) mentions the national combating terrorist activities system (sub-paragraph 2, Part Three, Article 4), while the Resolution of the Cabinet of Ministers of Ukraine, dated 18 February 2016, approved Regulation on integrated state system for prevention and cessation of terrorist attacks and minimization of consequences thereof (Cabinet of Ministers of Ukraine, 2016). Concurrently, the Law of Ukraine "On National Security of Ukraine" (Law of Ukraine, 2018) requires a review of the national combating terrorism system (par. 5, Article 27), and the President of Ukraine (2019b) approved the national combating terrorism system review procedure.[27]

Functions of the State Service of Special Communication and Information Protection of Ukraine in the sphere of cybersecurity were extended by the Law of Ukraine "On the Foundations of the Cybersecurity of Ukraine" (Law of Ukraine, 2017), while the subject-matter Law of Ukraine "On the State Service of Special Communication and Information Protection of Ukraine" (Law of Ukraine, 2006) sets out the functions and tasks of this state authority solely in the sphere of cyber protection. These legal conflicts must be resolved.

The system of strategic planning in Ukraine does not currently provide clear mechanisms for coordinating all processes of preparation of strategic and program documents at the national, regional, and local levels within a single cycle. A similar situation exists in the sphere of emergency response planning. The lack of systems approach to risk management and ensuring preparedness

[27] The collision is to use different names of the same system in different regulatory acts.

significantly hinders prioritization in the areas of development of the state and strengthening national resilience.

Ukraine, like most nations across, faced many challenges with regard to the spread of COVID-19, such as:

- the inability of early detection, evaluation, and prevention of new and hybrid threats;
- the lack of capabilities, reserves, and alternative strategies in case of emergency;
- absent or irrelevant comprehensive threat response plans, uniform standards, and protocols of concerted actions (in particular, regarding the introduction of restrictive measures in quarantine) at the national, regional, and local levels;
- inadequate level of medical and law enforcement personnel preparedness to act in emergency and quarantine restrictions;
- unpreparedness of state authorities, most enterprises, and the population to work under quarantine restrictions, including remotely;
- slow response by the authorized state and local bodies of anti-crisis management, low efficiency of coordination of efforts at various levels, including due to shortcomings in the legislation;
- inefficient strategic planning and analysis system in the state, incl. comprehensive assessment impact of threat and response measures on different areas of national security, monitoring of response effectiveness. (Reznikova, 2020b).

The problems, identified during the spread of COVID-19, were proof of the Ukrainian crisis management system's inefficiency, and also existing considerable vulnerabilities across various spheres (primarily healthcare, biosafety, economy). This highlights the increasing importance of taking measures to strengthen the national resilience on a system basis to generate the ability of society and the state to counter threats of various origins, adapt rapidly to the changing security environment, maintain sustainable operation, and also prompt recovery after the crisis toward an optimal equilibrium under defined conditions.

There are other problems that were revealed during the spread of the COVID-19 crisis and the aggression of Russia against Ukraine that began in 2014, and which need to be addressed by building up the national resilience ensuring system, such as:

- insufficient level of ensuring preparedness for response and cooperation between state authorities and civil society in crises and of maintaining an appropriate level of security of vital functions of the state;
- the lack of universal procedures and protocols of concerted actions with regard to the anticipation, prevention, and response to risks and crises at various phases of their evolution (particularly taking into account inter-sectoral interdependencies and potential cascading effects), and also recovery plans for sustainable functioning;
- the lack of uniform methodological principles to assess national security risks and the status of relevant capabilities to set substantiated priorities of the public policy in national security and in the sphere of drafting, adoption, and implementation of strategic decisions;
- inefficient mechanisms of organization and coordination of efforts in crisis management at the national level;
- the technical, moral, engineering, and material obsolescence of public administration system, primarily with regard to the ensuring of civil protection;
- inadequate level of public awareness and awareness of personnel of state and other entities with regard to specific manifestations and impacts of various risks and threats, or how their prevention and response mechanisms work;
- insufficient level of public trust in state authorities and the resulting insufficient level of engagement of population and civil society institutions in the implementation of national security and resilience ensuring measures;

- lack of bilateral channels of communication and lack of communication between central and local authorities and the population.

In general, the implementation of systems mechanisms of ensuring national resilience in Ukraine will require, first of all, legislative regulation of organizational framework to support the functioning of the relevant system, including specification of the powers, tasks, and responsibilities of national resilience ensuring actors, including central and local authorities, enterprises and organizations, as well as responsibilities of civil society entities, and procedures for various actors during peacetime, in emergencies and during martial law.

5.3.4. Gaps in the System of Risk and Capability Assessment in Ukraine

The current *Ukrainian legislation does not determine full planning cycle in the sphere of national security*, which should entail regular analysis and assessment of risks, evaluation of security capabilities, identification of threats and vulnerabilities, planning of measures to ensure resilience of the state, branches and areas, regions and local communities, as well as of society, and drafting of strategic and policy documents of the state. Most of these processes are not harmonized, while some have not been regulated as such (Reznikova et al., 2020).

Presently Ukraine's ministries and agencies assess risks and threats in their areas of responsibility using different methods, criteria, and approaches. The main problem is that it is difficult or sometimes impossible to compare the outcomes of such assessment obtained in this manner. This makes it impossible to objectively rank threats, assess their interactions, identify possible cascading effects, does not contribute to the unbiased setting of goals and objectives of state policy in national security.

The lessons of the 2020-2021 development of the strategies in the areas of national security of Ukraine showed that not all state authorities of Ukraine paid sufficient attention to the analysis of security environment and risk assessment, and focused on the issues relating to their daily routine. It should be noted, that it is common practice in the world to have this important work fulfilled by research institutions at the request of national or local authorities. What complicates the situation even further is that the state body responsible for organizing and coordinating actions in the relevant field has not been identified yet.

Up-to-date methods and techniques of risk and threat assessment, simulation of crises, forecasting, generation of multi-criteria matrices of threats, data catalogs, geospatial data analysis, and "smart" city technologies have not been promoted yet. The existing methodology gaps in the past event-based risk assessment produce less accurate forecasts, as they fail to reflect new challenges that have not been observed before. This was proven in the case of the COVID-19 spread and hybrid threats effects. The use of methods in projections relying mostly on expert opinions reduces the objectivity of such projections and hinders adaptation of national systems and processes in the area of ensuring national security to functioning in uncertainty.

The process of comprehensive review of the national security and defense sector and its components is also deficient. According to par. 1, Article 1, Law of Ukraine "On National Security of Ukraine," a comprehensive review of the national security and defense sector is a procedure of evaluation of the status and preparedness of national security and defense sector actors to accomplish their assigned tasks. Based on the results of such evaluation, the conceptual documents related to national security and defense sector components development, and measures supporting the attainment of their required capabilities to accomplish specified tasks in the current and projected security environment have to be drafted and refined (Law of Ukraine, 2018). Article 27 of this Law sets out a general procedure of comprehensive national security and defense sector and its components reviews. The comprehensive review methodology has not been specified, thus allowing for potential inconsistencies in methodology during a review of specific sub-systems of Ukraine's national security and defense sector (defense, public security and civil protection, defense industrial complex, intelligence agencies of Ukraine, National Counter-Terrorism System, cybersecurity of government information resources, and critical information infrastructure), and when comparing their results. Inter-agency cooperation in this sphere and consideration of research results are insufficient. The lack of definitions and methodology makes it difficult to understand how fully such reviews evaluate capabilities needed to ensure national resilience, including those in certain areas and branches.

As of August 1, 2021, the following reviews in the areas of national security of Ukraine were completed:

- defense review - the report on this review was approved by the President of Ukraine (2020c);
- review the intelligence agencies of Ukraine - the report on this review was approved by the President of Ukraine (2021h);
- review of national counter-terrorism system - the report on this review was approved by the President of Ukraine (2021k);
- defense industrial complex review - the report on this review was approved by the President of Ukraine (2021e).

The following requirements of the Law of Ukraine "On National Security of Ukraine" were not met timely:

- the public security and civil protection review: the President of Ukraine (2020d) recognized that the efforts of competent authorities were insufficient, and Ukraine's Ministry of Interior was assigned to complete the review within three months (before 29 March 2021) and duly refer a report for the review to the NSDC of Ukraine;
- review of the cybersecurity status for critical information infrastructure, government information resources, and information that is required to be protected by the legislation: although the review procedure was approved by the Cabinet of Ministers of Ukraine (2020c), the review has not been completed in time, and Decision of the NSDC of Ukraine, enacted by the President of Ukraine (2019c), is still pending. However, the Cybersecurity Strategy of Ukraine ordered the development and approval of annual national cybersecurity system status review procedure (President of Ukraine, 2016b).

Therefore, it can be stated that the objectives of the National Security Strategy of Ukraine (2020) regarding generation of planning documents in the areas of national security, based on the findings of comprehensive review of the security and defense sector, sectoral and other reviews in accordance with the defense and security reform towards NATO norms, principles, and standards (par. 58 of Strategy) have not been accomplished in full scope. The lack of expected outcomes in the areas of public security and civil protection, and cybersecurity of critical information infrastructure, government information resources, and information that is required to be secure by law, impedes the security reform. In addition, the fact that some review reports were approved later or almost simultaneously with the adoption of documents regarding planning in relevant national security areas raises concerns. This may signify that the review findings were not fully considered in strategic planning.

Organizational and analytical elements of the integrated network of situational centers, including those engaged in risk assessment, early threat detection and prevention, and identification of vulnerabilities, need to be developed.

The NSDC of Ukraine’s Decision, enacted by the President of Ukraine (2015a), established the Main Situational Center of Ukraine as a software and hardware complex for information collection, storage, and processing to support decision-making processes in the sphere of national security and defense. The functioning of the Main Situational Center of Ukraine is supported by the NSDC Staff. According to the adopted decision, the Main Situational Center of Ukraine shall obtain information (including in the remote mode) from the Ministry of Defense of Ukraine, Ministry of Interior of Ukraine, Ministry of Foreign Affairs of Ukraine, State Fiscal Service of Ukraine, State Emergency Service of Ukraine, Administration of the State Border Guard Service of Ukraine, other central executive authorities, Security Service of Ukraine and intelligence agencies of Ukraine.

Certain problems emerged at the stage of establishing the Main Situational Center of Ukraine with regard to determining the information assessment criteria, methods of analytical processing thereof, and building up analysis models. Domarev (2017) particularly pointed this out. To a large extent, this situation resulted from an incorrect legal definition of the Main Situational Center of Ukraine as a "software and hardware complex." In this regard, the Main Situational Center of Ukraine was not covering such important functions as analysis, information sharing, projection and simulation of crises, early warning, and other roles that are commonly performed by the relevant entities in developed countries, thus needing a comprehensive reform. The problems of methodological, organizational, and regulatory character, inter alia, significantly hindered the processes of development and implementation of universal threat and crisis response protocols to effectively respond to a broad spectrum of threats.

In June 2021 Decision of the National Security and Defense Council of Ukraine[28] set out a range of measures concerning the development of the situational centers' network, improvement of reliability, incorporation of up-to-date digital technologies, establishment of reserve capabilities, information sharing alignment, strengthening of cybersecurity, and information protection. According to this NSDC's Decision, this extended network of situational centers shall consist of the Main Situational Center of Ukraine, the Government Situational Center, situational centers of security and defense sector entities, situational centers of central executive authorities, the Cabinet of Ministers of the Autonomous Republic of Crimea, the regions, Kyiv and Sevastopol cities administrations, and also a back-up and mobile situational centers.

Analysis of measures, as specified in the subject document, allows for the conclusion that they target the strengthening of resilience of both, the network

[28] President of Ukraine. *Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 4 chervnia 2021 roku «Shchodo udoskonalennia merezhi sytuatsiinykh tsentriv ta tsyfrovoi transformatsii sfery natsionalnoi bezpeky i oborony»* [On the decision of the National Security and Defense Council of Ukraine of 4 June 2021 "On improvement of the network of situational centers and digital transformation of the sphere of national security and defense"]. Decree of the President of Ukraine of 18 June 2021 No 260/2021. Retrieved from https://www.rnbo.gov.ua/ua/Ukazy/4916.html.

itself and the national resilience in general, particularly in the area of ensuring the reliable and continuous functioning of public administration system, including during martial law, emergency and crisis, which jeopardize the national security of Ukraine. Meanwhile, some issues regarding the organizational and analytical support of the network of situational centers in Ukraine remain unregulated. It should be noted, that collection and analysis of the necessary input information and the results of their processing using special software packages in the network of situational centers requires the involvement of specialists with high levels of training and experience in analytical work in the field of national security. This raises the issue of improving the educational programs for personnel of Ukraine's security and defense sector, as well as creating the right motivation to attract high-quality professionals to work in state authorities and public institutions.

As for the planning system for the response to certain threats and emergencies in Ukraine, it is quite advanced. Different types of plans are developed, such as emergency response plans and civil protection plans at different levels, plans of cooperation between government actors and civil protection forces (Cabinet of Ministers of Ukraine, 2017b), mobilization plans, and plans for a martial law. The planning takes place throughout Ukraine, branches, regions, cities, districts, amalgamated local communities, and businesses. Meanwhile, the *Ukrainian legislation makes no provisions for planning for crises that go beyond emergencies and traditional threats and require cooperation between numerous national and local authorities*. This is mostly caused by the lack of regulatory framework supporting the prevention and response to crises, including preparedness ensuring action plans.

In particular, the definition of "crisis" is only provided in the footnote to the Law of Ukraine "On the National Defense and Security Council of Ukraine" in Article 4 (Competence of the National Security and Defense Council of Ukraine). It is noted in the Law of Ukraine (1998) that in case of crises jeopardizing the national security of Ukraine, the National Security and Defense Council of Ukraine has to coordinate activities of executive authorities, review proposals concerning the applicability of special economic and other restrictive measures (Part 2, Article 14); the Public Security and Civil Protection Strategy of Ukraine is the basis for the development of operational plans and plans for the use of forces and capabilities in crises (Part 3, Article 29).

Thus, the functions and objectives for components and actors of the security and defense sector and other state authorities in the sphere of ensuring preparedness and response to crises are not defined, as well as the coordinating body that would provide unity of approaches to the crisis planning and response, coherence of plans to ensure preparedness of different state authorities, including within the framework of the functioning of national systems.

Based on the analysis of Ukrainian legislation and existing practices in the sphere of risk and capability assessment, as important areas of ensuring national security and resilience, it can be concluded that the subject sphere faces the following key challenges:

- the holistic strategic planning system establishment in the state has not been completed;
- a lack of uniform methodology and techniques of comprehensive assessment of national security risks, evaluation of capabilities, identification of threats and vulnerabilities to determine the priorities of the public policy in national security and resilience, as well as substantiated strategic decision-making;
- a lack of a government authority responsible for organization and coordination of efforts in the sphere of national security threat and appropriate capability evaluation;
- inadequate legal regulation of the issues related to the planning and analysis in the sphere of national security within a uniform cycle, that includes, inter alia, national security risk assessment and evaluation of existing capabilities, as well as crisis response planning;
- insufficient inter-agency cooperation in this sphere and low level consideration of scientific research results;

- the lack of qualified personnel in the relevant area;
- limit of the resources.

The above challenges hinder the formulation of a balanced state policy in national security and resilience that is based on the results of comprehensive assessment of risks and capabilities, and identification of threats and vulnerabilities.

5.3.5. Problems of Ensuring Security and Resilience of Regions and Local Communities in Ukraine

The specifics of organization of activities and the practice of inter-agency cooperation and coordination in security area at regional and local levels, including response to and prevention of threats and emergencies, providing preparedness of the state and society, and post-emergency recovery efforts were studied in detail in Reznikova et al. (2021). In general, such activities in Ukraine rely upon basic legislation in the spheres of national security and civil protection, the subject-matter regulatory acts, and within the framework of the existing administrative territorial system. The Ukrainian legislation regulates the specifics of coordination and cooperation in the spheres of national security at national and territorial levels.

Presently the main responsibilities in prevention and response to threats and ensuring preparedness at regional and local levels are assigned to the region and district state administrations, self-government authorities of amalgamated local communities (ALC), territorial subdivisions of security and defense forces, and emergency medical services within existing national systems.

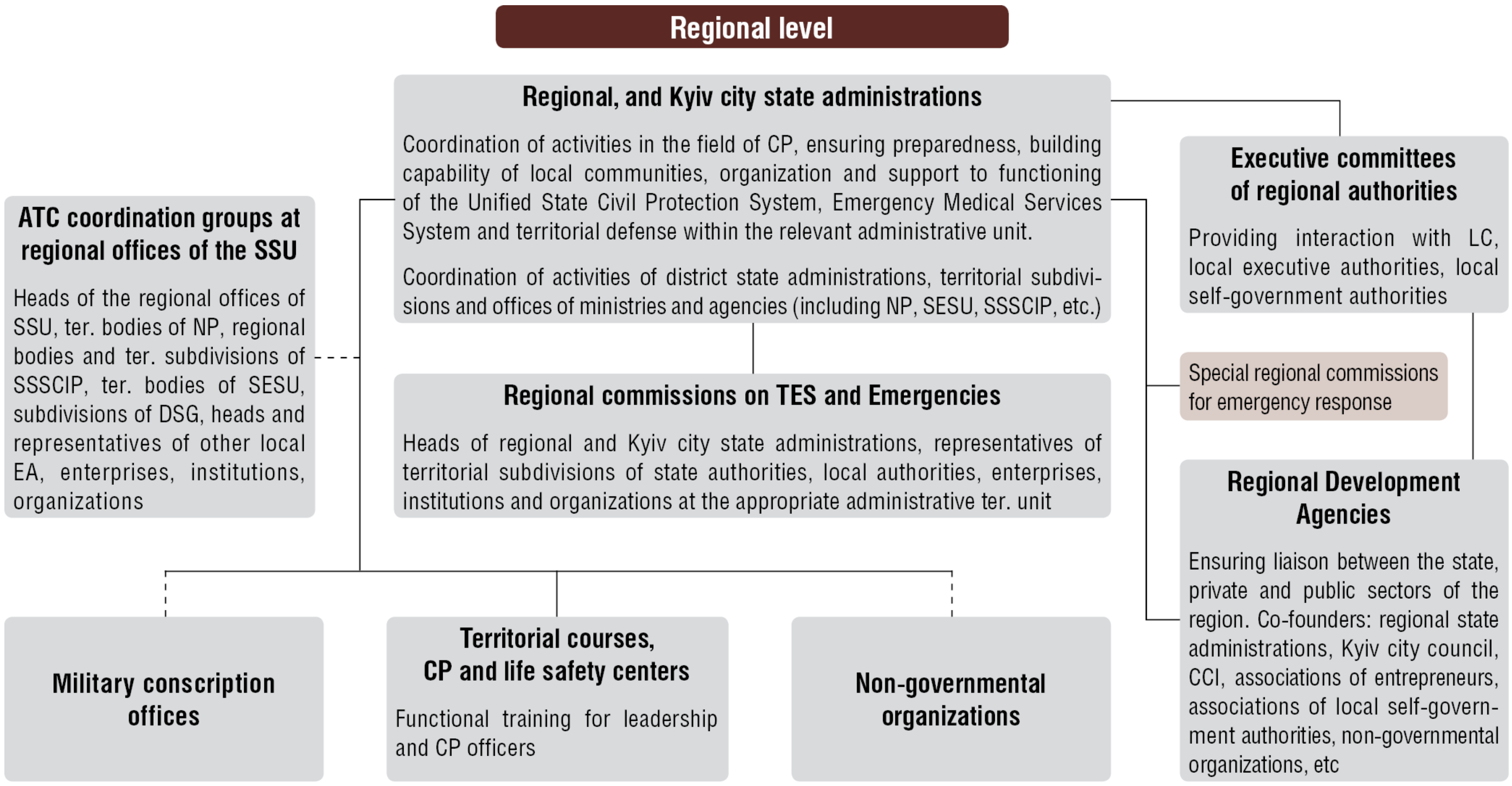
According to Ukrainian legislation, the main organizational formats of inter-agency cooperation in the field of prevention and response to certain threats and emergencies are established on a permanent or temporary basis at the regional and local levels, such as regional and local commissions on technogenic and environmental safety and emergencies; special commissions for emergency response at enterprises, institutions, and organizations; special post-emergency recovery commissions; Anti-Terrorist Center coordination groups at regional offices of the SSU; citizen safety centers. The following authorities will coordinate activities of the above inter-agency entities at the national level, as appropriate: the National Security and Defense Council of Ukraine, the Cabinet of Ministers of Ukraine, the State Commission on Technogenic and Environmental Safety and Emergencies, the Inter-agency coordination commission of the Anti-Terrorist Center under the Security Service of Ukraine, and others.

The local state administrations and local self-government authorities play an important role, within their competence, in coordination of activities in the sphere of civil protection, ensuring preparedness, building appropriate capabilities in local communities and territories, and in managing the functioning of national systems and territorial defense at the local level. The appropriate functions of these bodies are provided for by Ukrainian laws.

The national legislation regulates the organizational and legal mechanisms of cooperation between two or more amalgamated local communities (Law of Ukraine, 2014), public-private partnership (Law of Ukraine, 2010), and the engagement of volunteers and their organizations in addressing socially important issues (Law of Ukraine, 2011), including the ones in security area.

The citizen safety centers play an important role in ensuring preparedness and response to emergencies in local communities. They were established due to the changes occurring in Ukraine in connection with decentralization reform, reform of the State Emergency Service system, and transfer of specific emergency response powers from state to local authorities. Such centers combine the functions of protection from fires and other emergencies, public security, and emergency medical services supported by integrated communication and dispatch offices to coordinate the efforts. The establishment and effective operation of such infrastructure facilities in the security field requires coherent inter-agency cooperation in the sphere of emergency planning, risk analysis, and crisis management at the local level. In addition to providing rapid response to emergencies, citizen safety centers are to facilitate the improvement of safety culture in society, including through outreach programs.

Fig. 4.2. provides a general diagram of coordination and inter-agency cooperation in the sphere of national security at regional, local, and field levels. This diagram is based on direct and indirect linkages, as determined by Ukrainian legislation, between organizational formats (entities) of inter-agency cooperation existing in the subject area at different levels.



Regional level

Regional, and Kyiv city state administrations

Coordination of activities in the field of CP, ensuring preparedness, building capability of local communities, organization and support to functioning of the Unified State Civil Protection System, Emergency Medical Services System and territorial defense within the relevant administrative unit.

Coordination of activities of district state administrations, territorial subdivisions and offices of ministries and agencies (including NP, SESU, SSSCIP, etc.)

Executive committees of regional authorities

Providing interaction with LC, local executive authorities, local self-government authorities

Special regional commissions for emergency response

Regional Development Agencies

Ensuring liaison between the state, private and public sectors of the region. Co-founders: regional state administrations, Kyiv city council, CCI, associations of entrepreneurs, associations of local self-government authorities, non-governmental organizations, etc

ATC coordination groups at regional offices of the SSU

Heads of the regional offices of SSU, ter. bodies of NP, regional bodies and ter. subdivisions of SSSCIP, ter. bodies of SESU, subdivisions of DSG, heads and representatives of other local EA, enterprises, institutions, organizations

Regional commissions on TES and Emergencies

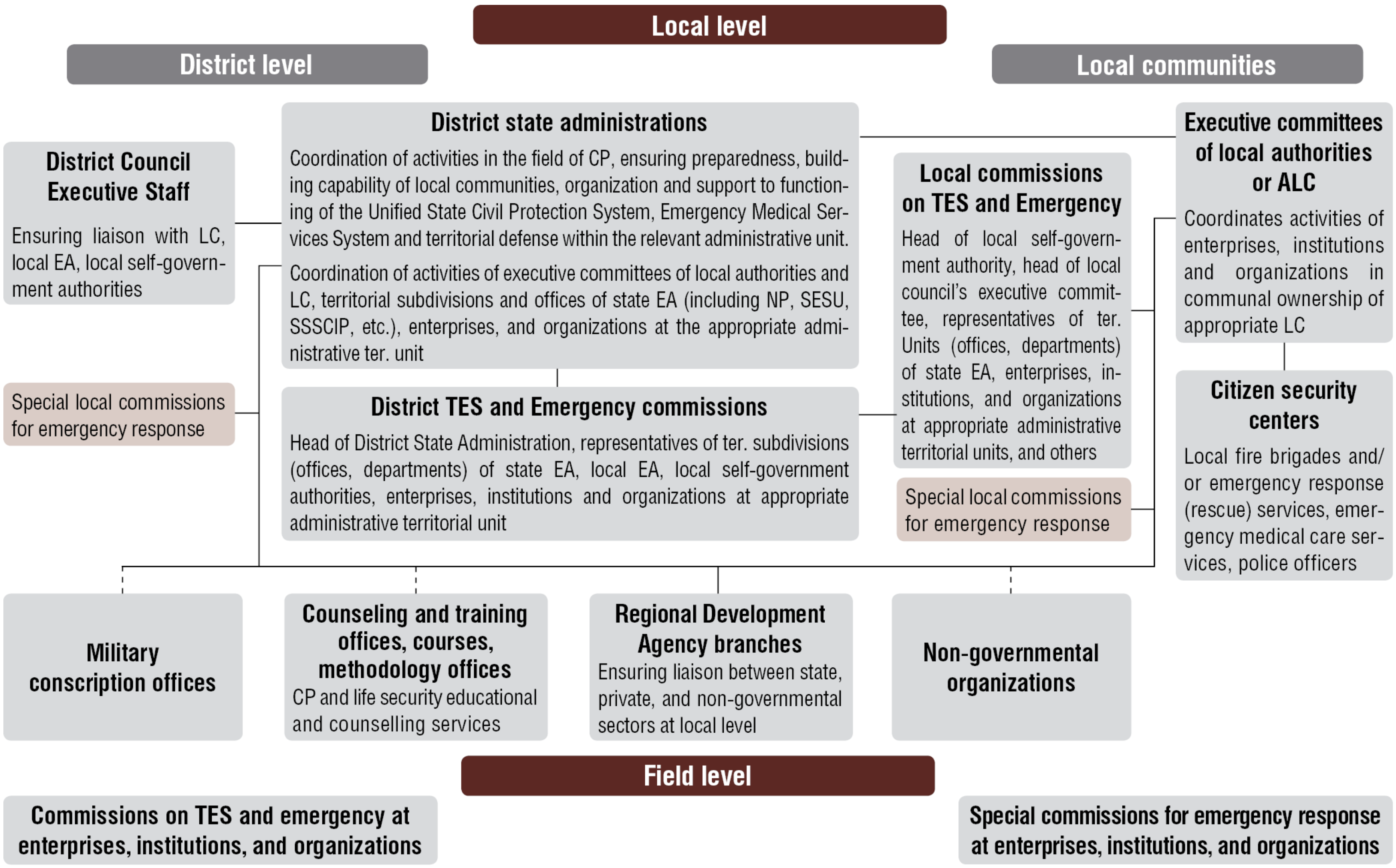
Heads of regional and Kyiv city state administrations, representatives of territorial subdivisions of state authorities, local authorities, enterprises, institutions and organizations at the appropriate administrative ter. unit

Military conscription offices

Territorial courses, CP and life safety centers

Functional training for leadership and CP officers

Non-governmental organizations



Local level

District level

Local communities

District Council Executive Staff

Ensuring liaison with LC, local EA, local self-government authorities

Special local commissions for emergency response

District state administrations

Coordination of activities in the field of CP, ensuring preparedness, building capability of local communities, organization and support to functioning of the Unified State Civil Protection System, Emergency Medical Services System and territorial defense within the relevant administrative unit.

Coordination of activities of executive committees of local authorities and LC, territorial subdivisions and offices of state EA (including NP, SESU, SSSCIP, etc.), enterprises, and organizations at the appropriate administrative ter. unit

District TES and Emergency commissions

Head of District State Administration, representatives of ter. subdivisions (offices, departments) of state EA, local EA, local self-government authorities, enterprises, institutions and organizations at appropriate administrative territorial unit

Local commissions on TES and Emergency

Head of local self-government authority, head of local council's executive committee, representatives of ter. Units (offices, departments) of state EA, enterprises, institutions, and organizations at appropriate administrative territorial units, and others

Special local commissions for emergency response

Executive committees of local authorities or ALC

Coordinates activities of enterprises, institutions and organizations in communal ownership of appropriate LC

Citizen security centers

Local fire brigades and/or emergency response (rescue) services, emergency medical care services, police officers

Military conscription offices

Counseling and training offices, courses, methodology offices

CP and life security educational and counselling services

Regional Development Agency branches

Ensuring liaison between state, private, and non-governmental sectors at local level

Non-governmental organizations

Field level

Commissions on TES and emergency at enterprises, institutions, and organizations

Special commissions for emergency response at enterprises, institutions, and organizations

Note: NP - National Police of Ukraine, SESU - State Emergency Service of Ukraine, SSSCIP - State Service of Special Communications and Information Protection of Ukraine, SSU - Security Service of Ukraine, DSG - Department of the State Guard of Ukraine, CCI - Chamber of Commerce and Industry, EA - executive authorities, LC - local community, ALC - amalgamated local community; CP - civil protection, TES - technogenic and environmental safety.

Fig. 4.2. **Diagram of coordination and inter-agency cooperation (at the level of existing organizational inter-agency cooperation formats) in the sphere of threat and emergency response at regional and local levels in Ukraine**

Source: Reznikova et al., 2021.

Analysis of existing inter-agency cooperation and coordination practice in security area at regional and local levels is a way to identify some challenges and hindrances in the course of building regional resilience and resilience of local communities.

The measures associated with ensuring resilience of regions and local communities in Ukraine are fragmentary and unaligned.

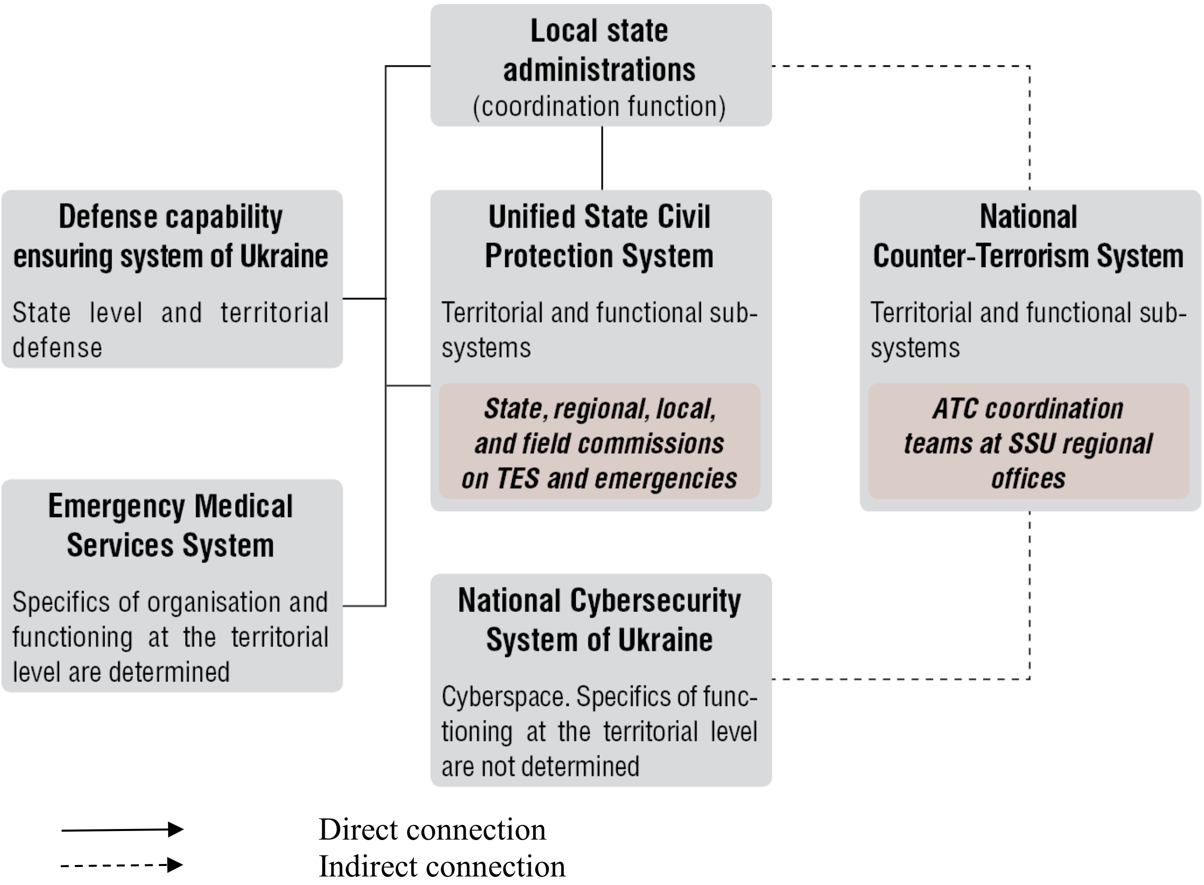
Conceptual and institutional ambiguity in the sphere of national resilience resulted in the inconsistent formulation of goals and objectives in ensuring resilience of regions and local communities. The Cabinet of Ministers of Ukraine (2020a) determined, in particular, the National Resilience System building at the regional level among its key objectives in the area of security infrastructure development within its operational goal 4, strategic goal 1 (Annex 2 to the State Regional Development Strategy during 2021-2027). However, no framework for the establishment of such a system was outlined in the Strategy. Moreover, the Concept of Support of the National Resilience System was approved in Ukraine next year after the adoption of the State Regional Development Strategy during 2021-2027. However, the State Strategy determined, inter alia, a number of measures facilitating the strengthening of regional resilience and resilience of local communities, including development of their security capabilities (citizen security centers, territorial defense forces, policing and crime prevention), generation of necessary reserves, critical infrastructure protection, establishment of the system of warning the population of threats or emergencies.

The *legislative and organizational support for the security and resilience of regions and local communities is inadequate.* This is related to the mechanisms of inter-agency cooperation and coordination of such efforts at different levels, clear vertical and horizontal linkages, public-private partnerships in security area, establishment of sustainable communication with the population.

At the level of local communities and regions, as well as in the state as a whole, there is no single comprehensive mechanism for coordinating activities within the full cycle of ensuring national resilience (situation monitoring, risk assessment, identification of vulnerability, ensuring preparedness, planning, response, post-crisis recovery). The organizational formats of inter-agency cooperation, existing in Ukraine, focus primarily on ensuring preparedness and response by competent authorities to certain types of threats (primarily terrorist and military ones) and emergencies. Vertical linkages between the center and regions have clear departmental (functional) orientation. This does not implement a comprehensive approach to countering threats of any origin at all stages and does not take into account the possible cascading effects of threats.

The organizational formats (entities) of inter-agency cooperation, established within the national systems for responding to certain types of threats and emergencies, functioning at the regional and local levels, partially intersect, and the mechanism for coordinating their activities is not defined. In particular, the regional and local commissions on technogenic and environmental safety and emergencies, and Anti-Terrorist Center coordination groups at regional offices of the SSU can be composed of representatives of approximately the same territorial state authorities and local self-government authorities according to the Civil Protection Code of Ukraine and the Law of Ukraine "On Combating Terrorism," (Law of Ukraine, 2003a, 2013a). However, the legislation does not establish required coordination of efforts or linkages between the existing national level systems and formats for inter-agency cooperation.

A general diagram of organizational linkages in the inter-agency cooperation framework in the field of response to threats and emergencies at the local level in Ukraine is presented in *Fig. 4.3*. As can be seen in the diagram, the key linkages between the national systems, which function at the regional level, are mainly facilitated by local state administrations having the function of control over most of the described above national systems at territorial levels. The National Cybersecurity System of Ukraine is an exception, given that its key domain is cyberspace, where the accent on territorial levels is no matter in principle. Meanwhile, cooperation between central and local authorities is also in place within the framework of this system.


Local state administrations
(coordination function)
Defense capability ensuring system of Ukraine
State level and territorial defense
Unified State Civil Protection System
Territorial and functional sub-systems
State, regional, local, and field commissions on TES and emergencies
National Counter-Terrorism System
Territorial and functional sub-systems
ATC coordination teams at SSU regional offices
Emergency Medical Services System
Specifics of organisation and functioning at the territorial level are determined
National Cybersecurity System of Ukraine
Cyberspace. Specifics of functioning at the territorial level are not determined
Direct connection
Indirect connection

Note: SSU – Security Service of Ukraine, ATC – Anti-Terrorist Center, TES – technogenic and environmental safety.

***Fig.4.3.* Organizational links between main formats of inter-agency cooperation in the sphere of threat and emergency response at a local level in Ukraine**

Source: Reznikova et al., 2021.

The problem of inadequate inter-agency cooperation and coordination of efforts at different levels became apparent in Ukraine in countering the spread of

COVID-19, a major emergency with cascading effects (Reznikova, 2020b). According to Zhalilo et al. (2020), the ineffective inter-agency cooperation, including between the center and regions, as well as between neighboring regions and local communities, besides reducing the threat response effectiveness, also complicates development of resilience against epidemics/pandemics, which is primarily formed at the level of regions and communities. Another problem in this sphere is a lack of systemic sharing of information concerning all potential threats and emergencies, including at territorial and local levels established in Ukraine.

Interaction between state authorities and the non-governmental sector, civil society, and the population to ensure security and resilience, including at the level of regions and local communities, takes place in a very limited format, and the relevant strategic communications are not sustainable.

The capacity of existing inter-agency entities as platforms of vertical and horizontal inter-agency cooperation, and communication of businesses and non-governmental organizations with local authorities in developing effective regional policy and ensuring security and resilience of regions and territorial communities, is not used effectively. This particularly concerns the Inter-agency Coordination Commission for Regional Development, regional development agencies. The Communities and Territories Development Council's performance was found insufficiently effective. It was dissolved in early 2021, and the Congress of Local and Regional Authorities was established under the President of Ukraine with broader functions and powers (President of Ukraine, 2021l).

A lack of systems approach to risk management and ensuring preparedness substantially complicates comprehensive analysis of current and potential risks and threats and identification of vulnerabilities at the level of local communities and regions, decreases objectivity of planning and prioritization of their organizational and security capabilities development and strengthening resilience.

Currently, there is no practice of risks and capabilities assessment and identification of specific threats and vulnerabilities at the level of regions in Ukraine. Most documents concerning regional development do not provide goals and objectives regarding strengthening regional security and resilience. A lack of strategic vision of security environment development at regional and local levels and existing problems in the sphere of inter-agency cooperation and coordination complicate generation of joint capabilities and ensuring preparedness of local communities for cross-sector or hybrid threats, the consequences of which may have multi-vector cascading effects in different spheres. The weak mechanisms of crisis management and risk management at local levels reduce the effectiveness of initial response to threats and emergencies, which should be provided directly at the source of emergency.

A *range of problems exists in the organization and functioning of some national systems related to providing security and resilience at regional level*.

Firstly, there is a number of gaps in the organization and functioning of territorial sub-systems of the Unified State Civil Protection System and its elements, such as regional and local commissions on technogenic and environmental safety and emergencies. Thus, according to sub-par. 4, par. 5, Standard Regulation, approved by Resolution of the Cabinet of Ministers of Ukraine[29], the subject commissions may involve representatives of territorial subdivisions of state authorities, local executive and self-government authorities, enterprises, institutions, and organizations, located in appropriate administrative territorial units (as agreed upon with their leadership). According to sub-par. 3, par. 6 of the mentioned document, the commission's composition shall be approved by the founding body, as proposed by subdivisions of state authorities, local executive and self-government authorities, enterprises, institutions, and organizations, located in appropriate administrative territorial units.

Therefore, engagement of representatives of the Security Service of Ukraine, Armed Forces of Ukraine, and other military agencies' territorial subdivisions is not provided by the legislation. However, this possibility is

[29] Cabinet of Ministers of Ukraine. *Pro zatverdzhennia Typovoho polozhennia pro rehionalnu ta mistsevu komisiiu z pytan tekhnohenno-ekolohichnoi bezpeky i nadzvychainykh sytuatsii* [On approval of Standard Regulation on technology-related/ecological safety and emergencies commission]. Resolution of the Cabinet of Ministers of Ukraine of 17.06.2015, No 409. Retrieved from https://zakon.rada.gov.ua/laws/show/409-2015-%D0%BF#Text

appropriate given the need for constant forecasting of the possible spread of the emergency and the scale of its consequences, ensuring preparedness to act in an emergency, continuous monitoring of the development of the emergency and the situation at affected facilities and adjacent territories.

The main tasks of the commissions at relevant administrative territorial units, as specified in par. 3 of the subject Standard Regulation, should encompass a number of important areas in terms of ensuring preparedness to respond to emergencies and establishing effective inter-agency cooperation, including the following:

- comprehensive assessment of risks of emergencies, forecasting of potential cascading effects;
- shared situational awareness across appropriate administrative territorial units;
- availability of joint concerted action plans for emergency response;
- facilitation of inter-agency exercises and training;
- control of preparedness status.

Correspondingly, among the powers of commissions, as specified in par. 4 of Standard Regulation, some important areas are missing, such as:

in daily activities:

- facilitate a continuous comprehensive analysis of emergency risks in administrative territorial units and disseminate the results of such analysis among members of commissions;
- coordinate development of universal plans and protocols of concerted actions in an emergency by territorial subdivisions of state authorities and local self-government authorities;
- acquaintance with the dynamic of reserves generation and its state, and additional capabilities needed in case of emergencies, as well as emergency response plans, as reported by representatives of territorial subdivisions of state authorities and local executive and local self-

government authorities, and enterprises providing critical services to the population;

- acquaintance with the security, safety, and resilience measures in place, as reported by critical infrastructure facility owners/operators; initiate inspections of such infrastructure operational status to ensure its smooth functioning on high alert, and in case of emergency;
- foster inter-agency emergency response exercises and training sessions;

on high alert and in case of emergency:

- ensure cooperation with appropriate Anti-Terrorist Center coordination groups at regional offices of the SSU;
- engage, if necessary, representatives of other territorial subdivisions of state authorities, enterprises, and organizations that were not members of the commission previously.

Secondly, there are several number of gaps in organization of territorial sub-system of the National Counter-Terrorism System, hindering inter-agency cooperation and coordination of appropriate activities at territorial level. Thus, regulatory acts in the sphere of combating terrorism do not clearly identify authorities, institutions, organizations, as appropriate territorial sub-system actors. At the same time, it is defined that the organization of activities to prevent, respond to, stop of terrorist acts and minimize their consequences is carried out by the territorial sub-system actors. However, the Law of Ukraine (2003a) clearly sets out and designates state authorities as actors, directly combating terrorism under their mandate, and those, which can be involved in the prevention, detection, and cessation of terrorist activities, if necessary. Yet, this designation only concerns central authorities, and having no such designation of territorial bodies can complicate organization of these activities at regional and local levels.

In addition, there may be a problem with engaging representatives of the National Guard of Ukraine [NGU] and the Armed Forces of Ukraine [AFU] in Anti-Terrorist Center [ATC] coordination groups at regional offices of the Security

Service of Ukraine [SSU]. Ukraine's legislation (primarily the Laws of Ukraine "On National Guard of Ukraine" and "On Armed Forces of Ukraine") specifies the responsibilities of AFU and NGU's in countering terrorism. However, Article 4, Law of Ukraine (2003a) does not directly refer to AFU and NGU as terrorism combating actors, as opposed to the Ministry of Defense of Ukraine and the Ministry of Interior of Ukraine. In addition, Article 7 of the Law does not provide for NGU and AFU representation in ATC coordination groups at regional offices of the SSU.

The lack of legislative regulation on NGU and AFU representatives' engagement in ATC coordination groups at regional offices of the SSU assumes that such involvement is possible, but will require coordination with the Ministry of Interior of Ukraine and the Ministry of Defense of Ukraine. Yet, this ambiguity can hinder the process of terrorist threat prevention or response at local level. Thus, if it is necessary to involve representatives of the NGU or the AFU in an urgent meeting of the ATC coordination groups at regional offices of the SSU, a situation may occur when representatives of the NGU or the AFU will not be able to participate in such a meeting. This may negatively affect assessment of the security situation (including terrorist threat to AFU facilities, AFU and NGU forces and resources that may potentially be involved in counter terrorism operations in the region, or minimization and elimination of consequences of terrorist attacks, including the ones of man-made character), and also hinder immediate and adequate counter-threat efforts.

It should be noted, that ATC coordination groups at regional offices of the SSU are only established at the regional and the Kyiv city level. Upon that, the liaison between these teams and district state administrations, local self-government, local communities, and amalgamated local communities, as well as local commissions on technogenic and environmental safety and emergencies has not been clearly specified.

Thirdly, in view of existing problems with the Emergency Medical Services System functioning, a Concept of this system development (Cabinet of Ministers of Ukraine, 2019a), and an Action plan to implement the subject Concept (Cabinet of Ministers of Ukraine, 2020b) were developed and adopted. According to the Concept of Emergency Medical Services System Development, the main problems in the sphere of emergency response include the following: low capacity of this system to ensure timely provision of adequate medical care in case of emergencies or during emergency relief efforts; inefficient emergency response algorithms (including national and regional response plans, and medical facility response plans); the lack of an effective system of reservation of medicines, medical devices; inefficient inter-agency coordination and cooperation mechanism of responding to mass cases, including at the pre-hospital care phase. Also, the subject document recognizes that existing response plans fail to monitor and take into account actual information concerning the ability of healthcare facilities to rapidly increase the number of hospital beds and the number of patients receiving emergency medical care at the hospital care phase. Such ability involves both, available capabilities to accommodate patients and the required technical support to provide emergency medical aid to significant numbers of people. A number of technical problems have also been identified, which reduce the speed of arrival of emergency (ambulance) crews to the scene (including delayed processing of calls for emergency medical aid), and efficiency of liaison between emergency medical services actors and other rescue services (including the lack of autonomous radio communications, absence of clear models of coordination between the system's actors) (Cabinet of Ministers of Ukraine, 2019a).

Among other directions of emergency response improvement, the Concept of Emergency Medical Services System Development outlines the following:

- development and implementation of new emergency medical care organization methodology and medical triage of victims of mass cases at the pre-hospital stage (including the algorithm of cooperation between rescue services);
- establishment of permanent emergency response staffs at emergency medical care and disaster medicine operations control centers;

- development of the methods to estimate requirements in medications, medical supplies, vehicles for transportation, hospital beds, personnel, and volunteers;
- development of the methods to conduct joint training involving rescue services, state and local authorities, utility services, and volunteers (Cabinet of Ministers of Ukraine, 2019a).

Major effort in this area should have been taken during Phase 1 in 2019-2020, as specified in the Concept, including establishment and upgrade of operations control centers, telecommunication and information systems for operations control centers; autonomization of emergency medical care and disaster medicine centers; implementation of emergency medical services provision and medical triage of victims of a mass case at the stage of pre-hospital care methodology; improved inter-agency cooperation between the Ministry of Interior, the State Emergency Service and the Ministry of Health through medical training of their employees. The emergency caused by COVID-19 spreading has proven insufficiency of measures that were taken.

The implementation of the joint algorithms of emergency medical services, fire rescue, and police in medical emergency response efforts is scheduled for 2021–2023, while such time lag is unjustified considering the changing and uncertain security environment.

Therefore, improving the organization of national systems that operate in the field of national security at the regional level, taking into account the above proposals, will help not only increase the efficiency of their performance, but also the formation of systems links in the field of national resilience.

The problem of inter-agency cooperation in security area at regional and local levels can be a challenge for decision-making within existing organizational formats (including regional commissions on technogenic and environmental safety and emergencies, special emergency relief commissions, ATC coordination groups at regional offices of the SSU) due to the rigid chain of command, as set out by departmental regulatory acts and military regulations. The need to seek approval of higher authority at the ministry or agency in certain cases may lead to decision-making delays where a certain threat or emergency requires an immediate response.

Another problem of inter-agency cooperation may be the prevailing departmental approach to dealing with complex issues concerning ensuring security, resilience, and development of local communities and regions.

A solution to the subject problems can be development and implementation of universal protocols of concerted actions in response to threats and crises at different phases of their deployment.

The public-private partnership in the sphere of ensuring security and resilience of local communities and regions is currently underdeveloped.

The causes of this situation in Ukraine can include private sector's skeptical attitude to the potentialities of effective cooperation with local authorities, the low-level trust of citizens in national and local authorities, a lack of public awareness and outreach concerning the benefits and risks in the use of partnership mechanisms of this kind, weak security culture in local communities, which is based on voluntary involvement, self-organization, cooperation and joint responsibility principles.

The capacity of regional development agencies to stimulate public-private partnerships, employers' organizations and their associations, as well as volunteer organizations is used inefficiently.

The system of resilient bilateral strategic communication with the population at the level of local communities and regions has not been established.

Thus, public involvement in the drafting of regulatory acts, strategies, development plans, and plans for ensuring preparedness for emergencies and crises, which are significant for local communities and regions, has not become common practice. The population self-organization mechanisms, particularly in rural areas, are weak.

The system of technical communications is not developed. For instance, the functioning of the 112 emergency telephone number system to provide emergency assistance to people, although stipulated by the Law of Ukraine (2012), has not been set up.

The staffing of local executive and self-government authorities with qualified personnel, having experience in inter-agency cooperation in the sphere of national security and enhancement of preparedness of local communities for emergencies and crises, as well as in the establishment of public-private partnerships, needs to be improved.

The pending government decentralization reform creates risks for appropriate delivery of public services and complicates the processes of generation of the managerial and functional capability of local communities, including in the sphere of ensuring their security and resilience. According to Kovalivska, Barynova and Nesterenko (2020), this happens, inter alia, due to certain problems in the field of distribution of powers and responsibilities, areas of responsibility, and resources at local level. On the other hand, the COVID-19 crisis challenges the completion of decentralization processes and complicates the communications required for complex decision-making in this area (Zhalilo et al., 2020).

All of the above asserts that the mechanisms supporting integration of capabilities of adjacent amalgamated local communities into joint capabilities to ensure their security and resilience, established by law, have not yet been advanced sufficiently in Ukraine.

Conclusions to Chapter 4

Analysis of the current global security environment status and tendencies in its development gives the reason to describe it as highly volatile and uncertain. Hybrid threats of covert nature with non-linear effects have become common. Changes in the world result in the disruption of many existing connections and increase the number of vulnerabilities faced by most public relations actors. From the long-term perspective, the security environment in Ukraine will be considerably influenced by global development trends. One of the biggest long-term threats for Ukraine is the continued aggression of Russia that affects all spheres of activity.

Considering that current and potential risks and threats to Ukraine are dynamic and long-lasting in their character with probably major negative impacts on society and the state, making it unfeasible to overcome them completely, and also in view of existing vulnerabilities in the state and society and drivers of influence that can aggravate the situation (incomplete reforms, limited resources, difficult demographic, and social situation), building the national resilience ensuring system meets Ukraine's needs in the context of creating additional opportunities for ensuring national security.

Analysis of practices in the sphere of ensuring national security, crisis management, and public administration in Ukraine affirms that measures to ensure national resilience are fragmentary and non-systemic, and therefore, not effective enough. Inadequate subject-matter legislation and a lack of established institutional mechanisms and tools for ensuring national resilience significantly constrain the relevant processes, resulting in violation of key principles of national resilience ensuring. In addition, systemic process of national resilience ensuring in Ukraine is deterred due to low-level theoretical elaboration on the relevant problem.

Ukraine currently faces a range of problems with public policy development and implementation and setting of national resilience ensuring objectives, including in the fields of strategic planning, crisis management, and the planning of concerted efforts of comprehensive inter-agency nature to respond to crises.

Based on the findings of the analysis, it can be stated that inadequate legal regulation and lack of existing vertical and horizontal linkages complicate introduction of the uniform coordination mechanism within the framework of full national resilience ensuring cycle and the implementation of a comprehensive approach to counter a broad spectrum of threats and hazards, including those having potentially cascading effects, at all phases of crisis cycle. In addition, measures to ensure resilience of regions and local communities in Ukraine have fragmentary and unaligned character, the post-crisis recovery process is predominantly challenging, resource intensive, and lasting, low-level public-private partnership development in security area is observed, both at national and local levels, and resilient bilateral communications with the population have not been established.

Identified in this study systemic problems relating to ensuring national resilience in Ukraine, point to existing vulnerabilities of the state and society, and also, to the fact that these systems elements have not fully met most resilience criteria of state and resilience criteria of functioning.

It can be stated that, despite the substantial resilience potential of the state and society, systemic national resilience ensuring mechanisms have not been yet established to support adaptability of the state policy in national security and the management of key areas in providing essential services for the state and society in an uncertain and rapidly changing security environment, and roots evoking vulnerabilities in the state and society have not been eliminated completely. Dealing with the subject systemic problems in the sphere of ensuring the national resilience of Ukraine requires comprehensive settlement based on the systems approach and determinate conceptual framework rather than stand-alone measures in different areas.

Chapter 5
NATIONAL RESILIENCE ENSURING SYSTEM ESTABLISHMENT IN PRESENT-DAY UKRAINE

Strengthening national resilience is a priority of public policy in the field of national security in Ukraine. This is driven by the need to provide preparedness of the state and society to respond to a broad spectrum of threats of various origins, as well as to ensure continuity of the key processes in the country. Ukraine has considerable resilience potential, which is particularly confirmed by its experience in countering Russia's hybrid aggression. However, augmentation of security and defense force capabilities alone is not enough to build a full-fledged national resilience ensuring system in Ukraine. The appropriate systemic mechanisms are in their initial phase. Their establishment will foster reinforcement and development of the national security ensuring system of Ukraine. The selection of the general national resilience ensuring model should be based on the consideration of national interests, the needs for the state and society development, and specifics of Ukraine's security environment. The development of public policy in this area requires definition of goals, objectives, and guidelines along certain periods, as well as universal and special national resilience ensuring mechanisms, taking into account the regularities due to implementation of the resilience concept in the field of national security.

5.4. Conceptual Framework of National Resilience Ensuring in Ukraine

Considering the significant number of threats faced by Ukraine, the inadequacy of its national security ensuring system and public administration, as well as multiple vulnerabilities in the state and society, it would be expedient to establish an additional protective mechanism to strengthen resilience of the state and society. This concerns the multi-level comprehensive national resilience ensuring system related to the national security ensuring system of Ukraine. The conceptual framework for establishing a national resilience ensuring system in Ukraine can be determined by taking into account the results of security environment analysis, vulnerabilities of the Ukrainian state and society, and the regularities generated from the specifics of resilience concept implementation in the sphere of national security.

Vision. The national resilience ensuring system, which was developed on the basis of national interests and in consideration of the best world practices, functions on a permanent basis. This system is organized and operates at national, regional, and local (level of territorial communities) *levels*. Uniform resilience ensuring principles, processes, and mechanisms have been introduced at all levels.

The conceptual, terminological, methodological, organizational, resource-related, and other issues have been accommodated by Ukrainian legislation. Uniform standards, recommendations for ensuring national resilience, and adaptive management principles have been introduced and regulatory acts related to national security, civil protection, crisis management, strategic planning have been improved in consideration of national resilience and sustainable development principles. Coordination and coherence of effort of all actors at all phases of the national resilience ensuring cycle have been established. The elements of institutional and organizational support of the system include the following:

- national coordinator and the structure of its auxiliary bodies;
- general framework for distribution of powers and responsibilities of state authorities in their assigned national resilience ensuring areas;
- national network of competent public authorities and scientific institutions for strategic analysis and resilience related issues;
- standing organizational formats (entities) for cooperation between central and local authorities, non-governmental organizations, private businesses, and international partners regarding national resilience ensuring issues (at national and local levels).

The following function on a permanent basis:

- comprehensive national risk assessment system, which also includes crises projection and simulation, assessment of capabilities, identification of threats and vulnerabilities, visualization and dissemination of obtained results, and the monitoring and revision of risk assessments;
- systems for early threat detection and prevention based on an integrated network of situational centers and crisis management;
- regional and local resilience development networks and security centers.

Regular inter-agency exercises, training events involving the population, and other events to raise awareness and improve preparedness in responding to the broad spectrum of threats and crises are in place. Threat and crisis (including emergency) response and recovery plans are developed. The necessary and readily available reserves and capabilities across different areas have been established.

The functioning of the national resilience ensuring system provides for:

- a comprehensive approach to responding to a broad spectrum of threats and crisis situations at all stages of their deployment (monitoring, analysis and evaluation, planning of efforts, prevention, mitigation of potential consequences, countering, recovery);
- effective cooperation between government authorities (national security and the defense sector, as well as others), including real-time mode of applying advanced technologies, active engagement of communities, businesses, population in the joint threat prevention and response processes and relief efforts, and also coordination of such activities;
- high level of awareness of the population and officials regarding the character and relevance of threats, crises and other hazards, as well as appropriate action plans. This requires the promotion of necessary knowledge and skills among central and local authority representatives and population with regard to current and anticipated threats and response thereto, and building a safety culture in society;

- preparedness of the state and society to respond to any threats and ability to resist. This primarily concerns building appropriate capabilities and a coherent action plans in the case of a threat, or crisis (including emergency) occurrences, and recovery thereafter, appropriate exercises and training sessions;
- continuity of key processes supporting vital functions in society and state (governance, crucial services for society, business processes, and more);
- reliable and permanent channels of two-way communication between the government and the population, including continuously informing society of the evolving situation and measures that have been implemented with consideration of strategic communication objectives.

Mission. The main purpose of the national resilience ensuring system of Ukraine is to create (or enhance) the necessary capabilities and abilities of society and state to counter threats of a broad spectrum, to adapt to changing security environments, and to maintain sustainable operations, including through elimination of vulnerabilities, and to promptly recover after crises toward an optimal level of balance in the specified conditions.

Conceptual approach. Currently, Ukraine faces high level risks and threats practically in all spheres: internal and external, social, economic, political, military, and ecological. Multiple vulnerabilities exist due to an insufficient level of society consolidation, ineffective public administration, incomplete security and defense sector reform and decentralization processes, and systemic deficiencies in the national economy. Therefore, the conceptual principles of national resilience ensuring in Ukraine should be based on a broad approach and extend beyond the mere establishment of an effective crisis management system on the basis of civil protection and providing security for critical infrastructure facilities (Reznikova & Voytovskyi, 2020).

The emergency in Ukraine, caused by the COVID-19 spread, actualized the issue of strengthening national resilience, including the development of an appropriate legal framework and organizational system, as well as ensuring the government and society preparedness to respond to a broad spectrum of threats of different origins and continuity of main processes in the country (Reznikova, 2020b). Enhancement of economic and societal resilience, particularly with regard to information and other destructive influences, and also resilience of local communities and regions, is vital for Ukraine in the current circumstances. An important lesson of the COVID-19 crisis is that the implementation of anti-crisis measures should take into account all potential effects, including those that may have negative results from such measures, and that planning should be more flexible under uncertainty.

Key definitions. The launch of a number of new processes relating to building national resilience requires a uniform glossary of terms in the sphere of national security and resilience to be developed and introduced. This requires consideration of commonly accepted understanding of the national resilience concept and of the practices existing globally and in Ukraine (Reznikova & Voytovskyi, 2021). Taking into account the theoretical foundations, as described in the above chapters of this monograph, the definitions of “adaptability,” “preparedness of the state and society,” “hybrid threats,” “crisis,” “national resilience,” “national resilience ensuring mechanism,” “capabilities,” “resilience in certain spheres,” “national resilience ensuring actors,” “vulnerability,” and “national resilience ensuring cycle” have been developed (see the Glossary).

It would be expedient to create a national website to publish the commonly recognized national glossary of terms in national security and resilience spheres, and sectoral glossaries, including the ones relating to emergency management, as well as appropriate information and analytic papers. This will support consistency and conformity of terminology, common understanding of key terms and linkages between definitions, and will reduce the risk of communication errors.

National resilience ensuring principles. Considering the specifics of applying the national resilience concept in the sphere of national security, it is necessary to set forth the key principles based on which factor of the national resilience ensuring system of Ukraine should be built, such as comprehensiveness, inclusion (broad interaction), predictability, reliability, awareness, readiness, mobility, adaptability, redundancy, continuity, and subsidiarity.

The key national resilience ensuring areas. Considering the results of Ukraine's national security environment analysis, the existing vulnerabilities of society and the state, and problems with ensuring national security and resilience, the following key areas of providing national resilience in Ukraine can be identified:

- continuity of governance, including guaranteed efficiency and ability of authorities to perform their functions, and their organizational resilience;
- safety and security of critical infrastructure facilities, including
  - continuous operation of food, water, and energy supply systems;
  - continuous operation of transport systems, including providing prompt movement in crises;
  - cybersafety and cybersecurity of critical infrastructure facilities;
  - secure and continuous operation of communication systems;
  - ability of the healthcare system to operate under increased stress, including pandemics or high-casualty situations;
- civil protection in case of a threat, crisis, or emergency;
- ability to effectively respond to uncontrolled massive relocation of people;
- societal resilience, in particular, to information influences;
- financial and economic resilience, including continuity of major business processes and supply chains.

Other national resilience ensuring areas relevant for Ukraine include building resilience against destructive external influences, updating the conceptual framework and applying new counter-terrorism practices, and ensuring societal and national security. In general, it is expedient to implement resilience ensuring principles and mechanisms across all sectors and areas of activities. This is already happening in some areas, such as cybersafety, cybersecurity, and financial management.

Development of *education* takes on greater importance within the context of national resilience, including the training of personnel for security and the defense sector of Ukraine. Promotion of knowledge concerning up-to-date risks and threats and shaping *societal safety culture and models of responsible behavior* in society should start in pre-school and last a lifetime. Organization of training programs by authorized state bodies, output and distribution of visual products, training sessions for target audiences, and establishment of two-way channels of communication – all of these are crucial in ensuring preparedness of government and society to respond to threats and crises and further recovery.

Ukraine's security and defense sector authorities should focus more on increasing human capital at all phases, including selection of personnel, training, and purposeful occupational and refresher courses. Special focus should be on the motivation, professional relevance, appropriate patriotic education of employees, and continuous improvement of skills (Siomin & Reznikova, 2017). In addition, advancing cutting-edge technologies in the sphere of national security and resilience, including in the areas of cybersafety and cybersecurity, risk assessment and crisis simulation, require high-skilled personnel in different areas to be employed in security and defense sector.

The list of key areas regarding ensuring national resilience should not be final, it should be revised and extended according to the evolving security situation.

Key functions of the national resilience ensuring system. Considering the clauses of paragraph 47, the National Security Strategy of Ukraine 2020 (President of Ukraine, 2020b), and the conclusions presented above in this monograph, the key functions of the national resilience ensuring system in Ukraine should be defined as follows:

- assessment of risks, identification of threats and vulnerabilities, evaluation of capabilities and level of preparedness of the government and society to respond to threats;
- prevention of threats, minimization of negative influences, and mitigation of the impacts of threats or crises;
- providing preparedness for state and local authorities, institutions, enterprises, organizations, communities, civil society, and the population to respond to any threats and crises;
- ensuring adaptive management, including flexible planning and effective crisis management, particularly via the implementation of protocols of concerted actions to respond to threats, emergencies, and crises; recovery to reach at least the pre-crisis level of quality of life and functioning of the vital areas of society and the state activities; mandatory revision of plan based on the results of analysis of the dynamic of key parameters of the national resilience ensuring system and of security environment changes;
- establishment of effective coordination and clear cooperation between security and defense sector actors, other government authorities, local communities, businesses, civil society, and population in terms of prevention and response to threats and dealing with the consequences of crises;
- promotion of necessary knowledge and skills in the sphere of national security and resilience and shaping security culture in society;
- establishment and maintenance of reliable channels of communication between government authorities and the population;
- development of international cooperation on resilience related issues.

Expected results. The establishment and implementation of the national resilience ensuring system in Ukraine will help:

- to improve effectiveness of national security ensuring system and public administration;

- to ensure appropriate level of preparedness of the state and society to respond to threats to national security and crises of various origins at all phases of their deployment;
- to provide effective cooperation between all national resilience ensuring actors;
- to improve effectiveness of crisis management in the state;
- to reduce human, material, and financial losses in the case of threat or crisis of any type occurrence;
- to consolidate society and increase the level of public trust in the government;
- to increase capacity of local communities, develop local self-government in the context of preventing and countering threats and crises;
- to save the state's resources through their consolidation and efficient use;
- to enhance international cooperation, share lessons learned in the sphere of national resilience, and strengthen integration of Ukraine into the Euro-Atlantic security system.

It should be noted that these conclusions and recommendations were primarily incorporated into the Concept of Support of the National Resilience System, approved by the President of Ukraine (2021g).

5.5. Organizational and Legal Framework of National Resilience Providing in Ukraine

The formation of the national resilience ensuring system is a challenging mission, requiring the involvement of a broad network of government institutions, organizations, and numerous experts. Therefore, the primary definition of conceptual framework of this process will provide a shared vision of issues and objectives to be tackled, as well as the principles of a functioning of the relevant system.

The Concept of Support of the National Resilience System, approved by the President of Ukraine (2021g), is the foundation for systemic mechanisms and other regulatory documents in the subject area. In particular, the laws of Ukraine should specify the responsibilities of national resilience ensuring actors, and other legal documents will outline the requirements, recommendations, criteria, and indicators to evaluate the basic elements of the national resilience system.

Shaping such a legal framework provides for the drafting and adoption of a number of regulatory acts, including:

- amendments in legislative acts of Ukraine, such as the Law of Ukraine (2013a, 2018), and other regulatory documents concerning the organizational mechanism of a national resilience ensuring system, distribution of responsibilities, and coordination of relevant efforts;

- introduction of practices and methodology of risk assessment and identification of threats to national security, evaluation of existing capabilities and identification of vulnerabilities at national and regional (local) levels, as well as deciding on the formats for sharing the appropriate results;

- adoption of the Law of Ukraine on strategic planning, amendment of the Law of Ukraine “On National Security of Ukraine” and the Budget Code of Ukraine to establish a holistic strategic planning system with consideration of the budget process;

- amendment of legislative acts of Ukraine regarding planning in the spheres of national security, including improvement of joint action planning in the case of crises with complex cascading effects and the introduction of universal protocols for concerted response to threats and crises at different stages of their deployment;

- designation in Ukraine of regional and local coordination bodies for ensuring resilience of regions and local communities, establishment of organizational formats of broad cooperation at local levels operating on a permanent basis, and description of their powers in appropriate areas;

- installation of mechanisms to stimulate scientific research, building up of public-private partnerships in the sphere of national security and resilience, including description of obligations of public and private partners;

- designation of procedures, channels, and formats of information sharing between national resilience ensuring actors concerning current and expected threats, early signals of threats identification, the status of appropriate capabilities, identified vulnerabilities, as well as prevention, response, and post-crisis recovery plans, mechanisms, and procedures;

- identification of relevant target audiences and the introduction of the practice of regular exercises and training in the area of ensuring preparedness, and the response to threats and crises.

Currently, the expert community holds discussions on the expediency of drafting a specific basic law on ensuring national resilience as a basic law in the appropriate area. It should be noted, that the most critical issues concerning cooperation between the government and businesses in the area of providing security and protection of critical infrastructure, and definition of their responsibilities are regulated by the Law of Ukraine “On Critical Infrastructure” of 16 November 2021, No 1882-IX[30]. The remaining issues in the sphere of ensuring national resilience, including designation of powers and distribution of responsibility of actors, can be regulated through amendments in a number of subject-matter laws of Ukraine and appropriate decisions of the National Security and Defense Council [NSDC] of Ukraine and resolutions of the Cabinet of Ministers of Ukraine. In addition, the process of cooperation between national resilience ensuring actors should be determined in appropriate regulatory acts of Ukraine, including protocols of concerted actions setting forth universal threat and crises response and recovery procedures (algorithms). Thus, considering the above, drafting a separate law on ensuring national resilience is not expedient.

[30] Law of Ukraine. *Pro krytychnu infrastrukturu* [On critical infrastructure]. Law of Ukraine, 16 November 2021, № 1882-IX. Retrieved from https://zakon.rada.gov.ua/laws/show/1882-20#Text

The approval of the Concept of Support of the National Resilience System should be followed by a duly developed and endorsed action plan to support its implementation. Considering NATO recommendations, adopted by the 2021 Brussels summit, this plan should set out the appropriate goals and objectives, and include clear guidelines and their achievement indicators. In addition, the national resilience ensuring actors should incorporate the appropriate objectives and activities in sectoral strategies and concepts, relevant national and local level programs and plans outlining the key areas and tasks concerning the development and implementation of public policy in the fields of their responsibility.

A particular focus should be on the *organizational mechanism of the national resilience ensuring system,* mainly on coordination of appropriate efforts. As mentioned above, the distribution of constitutional powers between different institutions in Ukraine complicates the establishment of holistic functional national security and the resilience ensuring system, managed by an integrated center, thus creating inconsistencies and risks for the reliability of system organization and its balance.

Therefore, effective coordination of national resilience building efforts requires a clear format of cooperation between the Cabinet of Ministers of Ukraine and NSDC of Ukraine. The role of the Secretariat of the Cabinet of Ministers of Ukraine and the Staff of NSDC of Ukraine in coordination of activities in the field of national security and resilience should be enhanced, and special offices responsible for appropriate issues should be established within the structure of these bodies (Reznikova, 2020a).

Considering the distribution of constitutional powers between different branches of power in Ukraine and with regard to international practices, the mechanism of coordination of national resilience building efforts at the strategic level should be formed according to the conclusions below.

1. Considering the cross-cutting nature of resilience concept for ensuring national security, and the fact that the National Security and Defense Council of Ukraine is responsible for coordination in the sphere of national security, the

NSDC of Ukraine should provide the overall coordination of state policy in national security and resilience.

2. Since material, financial, and organizational capabilities are mostly concentrated in the executive branch of power, the Cabinet of Ministers of Ukraine should be responsible for the coordination of efforts of all potential participants in crisis management, including at the stage of ensuring preparedness to respond to the broad spectrum of threats and crises of different origins.

3. According to the Law of Ukraine (2013a), the Cabinet of Ministers of Ukraine establishes the State Commission on Technogenicand Environmental Safety and Emergencies to coordinate activities of central and local executive authorities, enterprises, institutions, and organizations in providing Technogenic and ecological safety, protection of population and territories, prevention and response to emergencies. According to the Cabinet of Ministers of Ukraine (2015), this State Commission is chaired by the Prime-minister of Ukraine. Therefore, the powers of this State Commission should be extended to include comprehensive planning of security measures at all phases (prior to, during, and after the crisis), and generation of necessary capabilities, as well as coordination of efforts in the sphere of ensuring security and the resilience of critical infrastructure. This can be a way to transform the State Commission on Technogenicand Environmental Safety and Emergencies into a governmental body for national resilience ensuring coordination.

4. To support the Ukrainian government's national resilience ensuring efforts and operation of the aforementioned State Commission (the governmental coordination body), it is appropriate to establish a Government Office under the Secretariat of the Cabinet of Ministers of Ukraine with the following responsibilities vested therein:

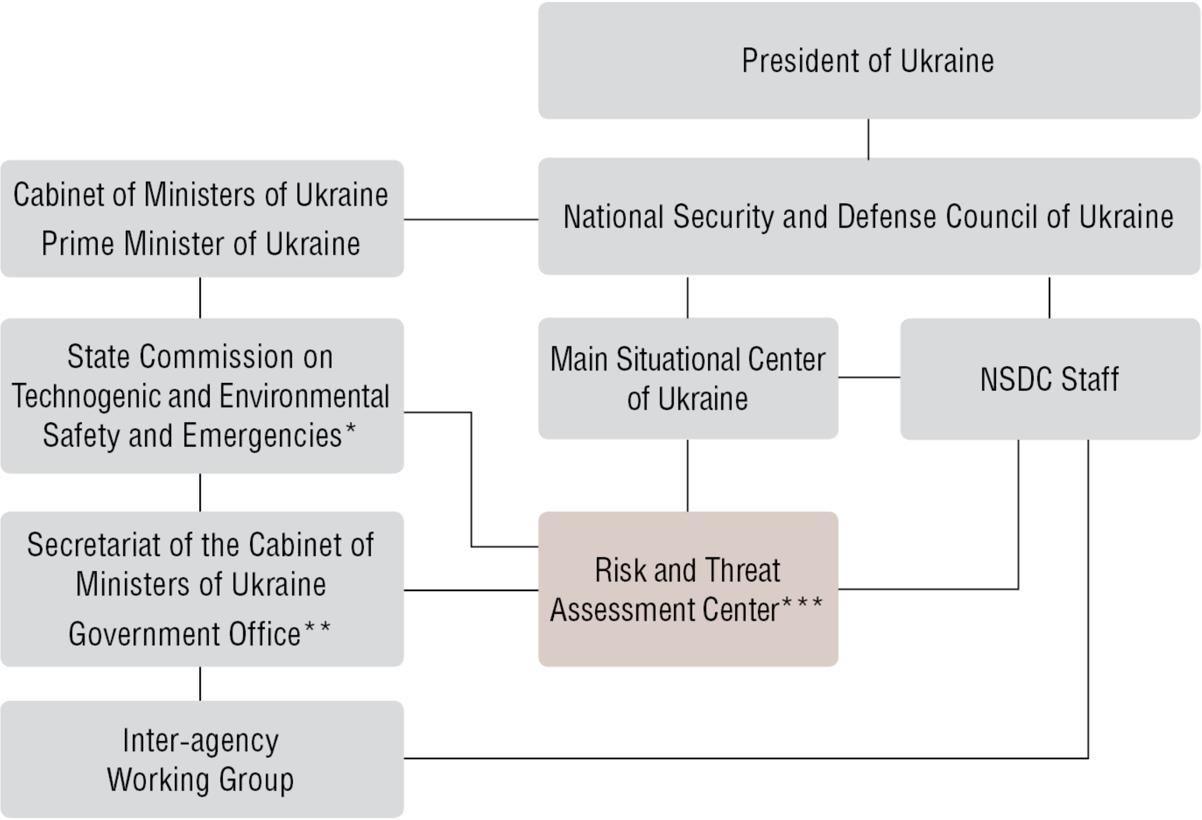
- organization of drafting of regulatory acts, manuals, and recommendations regarding national resilience ensuring issues (both, general and specific) for various target groups (ministries and agencies, communities, population, and businesses);

- development of a public-private partnership in the national resilience ensuring area;
- organization of specific training sessions and exercises to promote the necessary knowledge and skills regarding threats and crises and response to them at different phases;
- creation of a resilient inter-agency communications, and networks of scientific institutions and representatives of the civil society on national resilience ensuring issues;
- control over the status of implementation of decisions taken in the relevant field.

5. The Inter-Agency Working Group that has already been established under the auspice of the Commission for Coordination of Euro-Atlantic Integration of Ukraine can be a supporting entity to coordinate activities of central executive authorities in the sphere of building national resilience.
6. The establishment of the Center under NSDC of Ukraine for organization of multi-level threat assessment, projecting emergencies and crises, and maintenance of the National Threat Register is required. The Center should interact with the Main Situational Center of Ukraine, accumulate information from authorized state bodies assessing threats within their competence, interested scientific and non-governmental institutions, apply advanced methods and technologies to threat assessment, and crises projection and more. This issue will be detailed below.

Schematically the mechanism of coordination of efforts in the sphere of national resilience in Ukraine at a strategic level is presented in *Fig. 5.1*. It should be noted, that in view of national specifics of constitutional powers distribution between the main branches of powers, this proposed mechanism is not ideal, but it can be implemented in the near future without a constitutional reform in Ukraine. If constructive cooperation is established between the NSDC of Ukraine and the Cabinet of Ministers of Ukraine, this mechanism can be rather effective.

The situation around countering the emergency caused by the COVID-19 in Ukraine affirmed the expediency to organize coordination of national resilience building in Ukraine in the proposed way, including the leading role of the Cabinet of Ministers of Ukraine and the State Commission on Technogenicand Environmental Safety and Emergencies in the sphere of crisis management and providing a whole-of-government approach to cooperation.


President of Ukraine
Cabinet of Ministers of Ukraine
Prime Minister of Ukraine
National Security and Defense Council of Ukraine
State Commission on Technogenic and Environmental Safety and Emergencies*
Main Situational Center of Ukraine
NSDC Staff
Secretariat of the Cabinet of Ministers of Ukraine
Government Office**
Risk and Threat Assessment Center***
Inter-agency Working Group

Notes:

** – functions and powers of the State Commission should be extended, and it may be transformed into a government body for the national resilience ensuring coordination;*

*** – Government Office, the responsibilities of which will include strategic planning, crisis management, and national resilience ensuring issues;*

**** – a body that is expedient to establish.*

***Fig. 5.1.* Coordination mechanism in the field of national resilience in Ukraine at strategic level**

Source: developed by the author.

In addition to coordination bodies at a strategic level, the national resilience ensuring organizational mechanism should include a permanently functioning system of national and regional level resilience coordination bodies and inter-agency cooperation formats (structures) at regional and local levels operating on a permanent basis, the network of analytical, expert, scientific, educational institutions and centers for resilience development, as well as effective cooperation of all national resilience ensuring actors.

Considering the above, it is advisable to list all key elements of the national resilience ensuring organizational mechanism to include the following:

1) *national level*:

- National coordinator for the national resilience ensuring issues as a part of the National Security and Defense Council;
- Government Office for national security and the resilience ensuring issues at the Secretariat of the Cabinet of Ministers of Ukraine;
- Government coordination body for national resilience ensuring issues;
- permanent structures for inter-agency cooperation in the field of national security and resilience (inter-agency working groups, commissions, etc.);
- state authorities within their competence;
- supplementary and advisory entities for national resilience ensuring issues;
- national network of analytical, expert, scientific, educational institutions and centers for resilience development;

2) *regional and local levels*:

- local state administrations;
- permanent inter-agency cooperation structures for ensuring security and resilience of regions and local communities;
- territorial subdivisions of state authorities, local authorities, enterprises, institutions, organizations, civil society entities, and citizens initiating or engaging in the national resilience ensuring processes;
- supplementary and advisory entities for regional resilience ensuring issues and resilience of local communities;

- regional network of analytical, expert, scientific, educational institutions, and centers for resilience development.

Schematically the national resilience ensuring organizational mechanism is shown in *Fig.* 5.2.

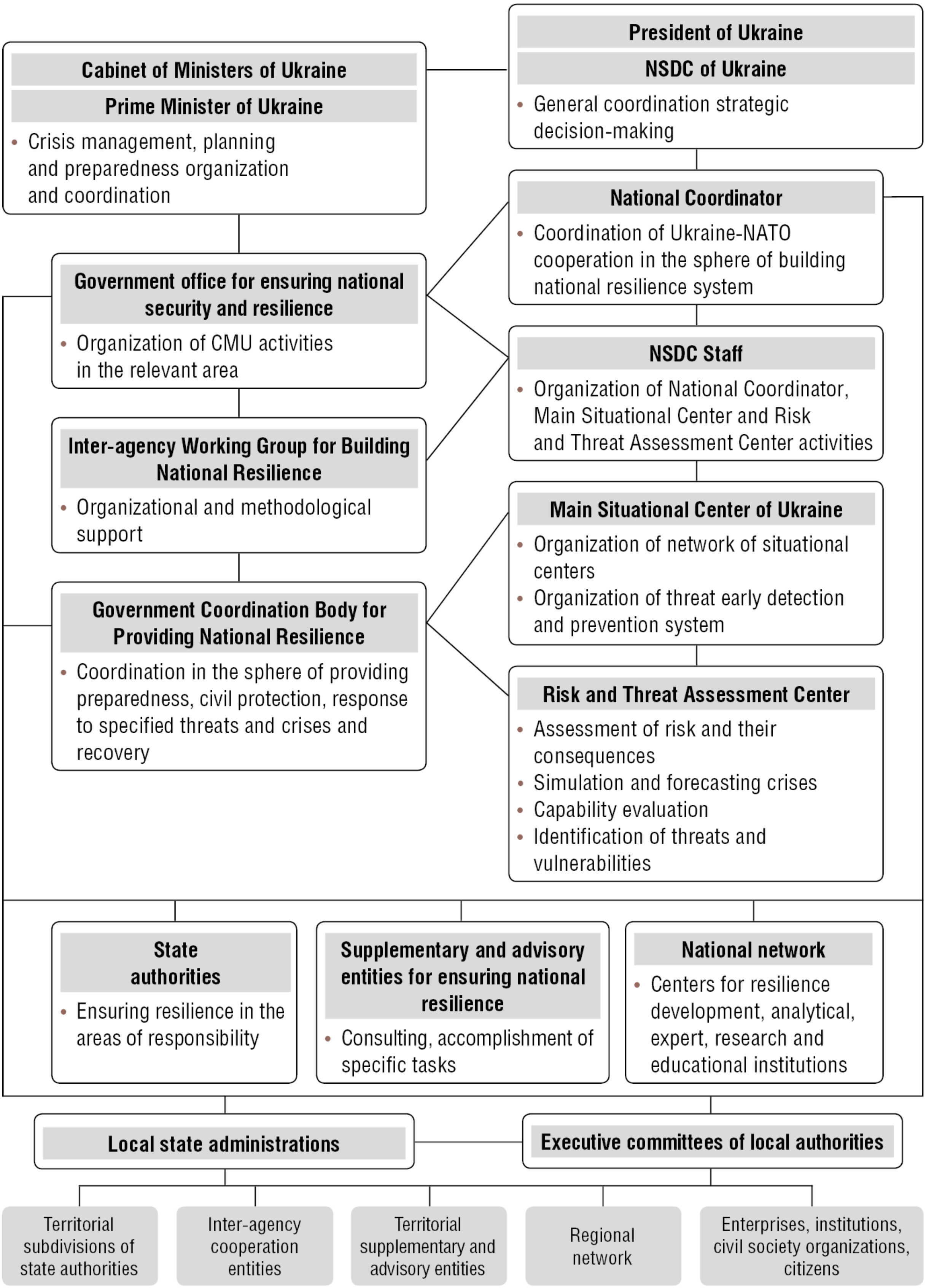

President of Ukraine
NSDC of Ukraine
General coordination strategic decision-making
Cabinet of Ministers of Ukraine
Prime Minister of Ukraine
Crisis management, planning and preparedness organization and coordination
National Coordinator
Coordination of Ukraine-NATO cooperation in the sphere of building national resilience system
Government office for ensuring national security and resilience
Organization of CMU activities in the relevant area
NSDC Staff
Organization of National Coordinator, Main Situational Center and Risk and Threat Assessment Center activities
Inter-agency Working Group for Building National Resilience
Organizational and methodological support
Main Situational Center of Ukraine
Organization of network of situational centers
Organization of threat early detection and prevention system
Government Coordination Body for Providing National Resilience
Coordination in the sphere of providing preparedness, civil protection, response to specified threats and crises and recovery
Risk and Threat Assessment Center
Assessment of risk and their consequences
Simulation and forecasting crises
Capability evaluation
Identification of threats and vulnerabilities
State authorities
Ensuring resilience in the areas of responsibility
Supplementary and advisory entities for ensuring national resilience
Consulting, accomplishment of specific tasks
National network
Centers for resilience development, analytical, expert, research and educational institutions
Local state administrations
Executive committees of local authorities
Territorial subdivisions of state authorities
Inter-agency cooperation entities
Territorial supplementary and advisory entities
Regional network
Enterprises, institutions, civil society organizations, citizens

Fig. 5.2. **National resilience ensuring organizational mechanism**
Source: developed by the author.

In the course of establishing the national resilience ensuring system the crisis response and post-crisis recovery procedures need to be harmonized, and effective cooperation and synergy of security and defense forces and existing or emerging national level systems in the sphere of national security (such as Unified State Civil Protection System, Emergency medical services system, Law enforcement system of Ukraine, National counter-terrorism system, National cybersecurity system of Ukraine, State system for critical infrastructure security) should be in place. In case of emergency occurrence, response thereto and relief efforts should take into account the requirements of the Code of Civil Protection of Ukraine, and threats should be addressed following the procedure set out in certain laws of Ukraine.

The correlation between the national resilience ensuring system and the national security ensuring system of Ukraine means that the key areas of responsibilities of ministries and agencies should remain unchanged, but their responsibilities in the national resilience should be determined, their cooperation procedure refined, and the local self-government's powers should be extended. It is not expedient to create new central government authorities. The issues of effective coordination and activities in the sphere of ensuring national resilience are recommended to be addressed by specifying the powers or through reform of existing entities without expanding the government apparatus.

This proposed way of the national resilience ensuring system organization in Ukraine envisages the cross-cutting implementation of national resilience principles across all spheres of national security, different areas of public policy, and public administration in general.

5.6. Specifics of Formation and Implementation of State Policy in National Resilience in Ukraine

5.6.1. Priorities of State Policy in National Security and Resilience

Public policy in the sphere of national security and resilience envisages the definition of key goals and objectives, as well as expected results and their evaluation criteria. According to the proposed above conceptual framework of building national resilience, the key objectives in this sphere in Ukraine should be formulated around the following ***general goals***:

- introduction of a new paradigm of thinking due to which ensuring national resilience is the responsibility of each citizen, not the government alone;
- development of an adaptive management model that requires flexible and multi-optional state policy in national security, availability of alternative goals and plans, regular public policy update based on changing security situations and development trends, introduction of purposeful self-government mechanisms;
- providing effective cooperation that requires implementation in practice of whole-of-government interaction and mutual support principles, establishment of partnerships between the state, businesses, and population, designation of areas of joint responsibility, coordination of state and regional policies, redistribution of responsibility to empower local authorities and territorial communities, facilitation of national, regional, and local leadership;
- ensuring social cohesion by uniting people around the issues of ensuring security and resilience within the state, region, and local community;
- development of security and other capabilities to provide an appropriate level of preparedness and effective response to the wide spectrum threats and crisis situations;
- improvement of planning through harmonization of security strategies and programs with relevant documents on social and economic development, formulate coherent action plans concerning prevention and response to threats and post-crisis recovery;
- building security culture in society – introduce the rules of behavior and skills relating to avoiding threats and hazards or minimizing their consequences for the state and society;
- ensuring effective civil control of state resources expenditures in the field of national security and resilience.

Considering the above goals, problems to be addressed in the sphere of national security and resilience in Ukraine, world experience, and regularities as specified in the national resilience concept, it is expedient to formulate the following ***key objectives*** in the sphere of building the national security and resilience ensuring system in Ukraine:

- improve Ukrainian legislation concerning ensuring national resilience, including designation of powers and responsibilities of various national resilience ensuring actors;
- establish national resilience ensuring multi-level organizational mechanism;
- set effective coordination and cooperation among state and local authorities, territorial communities, enterprises, organizations and civil society institutions with regard to national resilience ensuring issues;
- shape the system of national level and regional coordination bodies to address resilience ensuring issues, organizational formats of inter-agency cooperation to operate on a permanent basis, and the network of scientific, expert, educational institutions, and resilience development centers;
- establish a mechanism, including channels and formats, to share information among national security actors;
- improve the strategic analysis and planning system in the sphere of national security of Ukraine, including through the full-cycle strategic planning implementation;
- introduce various risk management practices at national level in Ukraine based on international standards (ISO, 2018a, 2019a), including mandatory risk assessment and capability evaluation procedures;
- create a comprehensive national risk assessment system that will also include crises projection and simulation, identification of threats and vulnerabilities, evaluation of capabilities, visualization and promotion of obtained results, monitoring and review of assessment, models and other results, etc.;

- develop and introduce criteria and indicators to evaluate resilience and preparedness of the state, society, and local communities, including resilience in specific areas, organizational resilience of state, local authorities, and strategic-level enterprises and organizations;
- improve crisis management procedures, including introduction of universal protocols of concerted actions in terms of prevention and response to threats and crises at different phases of their deployment, taking into account inter-sectoral interdependencies and potential cascading effects;
- develop and implement special national resilience ensuring mechanisms in certain areas;
- develop and implement special advanced training sessions and courses for civil servants, personnel of national security and defense sector with regard to ensuring national resilience;
- promote necessary knowledge among the population and develop skills regarding response to threats;
- stimulate public-private partnership in the sphere of national security and resilience;
- develop international cooperation in the sphere of providing resilience with the consideration of processes in the global and regional security environment.

Considering numerous complex tasks in the sphere of national resilience in Ukraine, the overarching national framework for the functioning of the national resilience ensuring system should be created at the initial stage (up to two years). During the next phase (up to five years) the relevant practices should be promoted to regional and local level through a pilot project in one region and several local communities.

In the long-term perspective (over five years), the required elements and sub-systems of the national resilience ensuring system should be developed and effectively function on a permanent basis. According to adaptive management principles, the goals and objectives in the sphere of national security and resilience should be reviewed and updated regularly, including with regard to the results of strategic analysis and comprehensive risk assessment.

The planning of measures related to building the national resilience ensuring system should envisage definition of expected outcomes and their evaluation criteria. Therewith, the outcomes, on one hand, can characterize the progress in implementation of the measures related to organizational and legal support of this system, and include adoption of relevant regulatory acts or the establishment of certain entities and formats. On the other hand, the measures that have been taken should demonstrate a positive dynamic of indicators characterizing the national resilience criteria. To that end, appropriate indicators should be developed for each specific national resilience ensuring area, taking into account general recommendations concerning resilience criteria formulation. At that, optimal levels of such indicators should be established as benchmarks according to the specific context of a situation. Periodically, benchmarks should be adjusted in line with the trends in the security environment and changes in the security situation and the key parameters of the national resilience ensuring system. The dynamic of actual indicators should be determined in the course of annual resilience self-assessment, as an important element of the comprehensive national risk and threat assessment system, which will be detailed below.

5.3.2. Improvement of Planning in the Sphere of National Security Taking into Account National Resilience Ensuring Goals and Objectives

The gaps in the strategic planning process in Ukraine were revealed in the course of major preparation of national security related documents in 2021, as required by the National Strategy of Ukraine 2020 (President of Ukraine, 2020b). Building national resilience ensuring system outlines new requirements to this process, which imply amendments in the Law of Ukraine (2018), to improve planning in the sphere of national security. It should be noted, that both the planning methodology and organization of appropriate processes in Ukraine need to be refined. The overall inconsistency of strategic documents and policy development processes in the state, including in the sphere of national security, economic and social development, and sustainable development actualizes the issue of development and adoption of the law on national strategic planning in Ukraine.

The main *principles* of planning in the sphere of national security and resilience should be as follows:

- lawfulness;
- objectivity;
- flexibility;
- cooperation;
- integrity;
- distribution of risks and responsibilities;
- reasonable transparency;
- coordination;
- control.

It should be noted, that planning is to become a part of adaptive management. Therefore, plans should be revised periodically and refined in line with up-to-date information. In particular, strategic planning processes, like other types of planning in the sphere of national security, should be aligned with risk and threat assessment.

Current Ukrainian legislation does not provide full-cycle planning in the sphere of national security, which should encompass periodic analysis and assessment of risks, security capabilities, identification of threats and vulnerabilities, planning of measures concerning providing security and resilience of the state, specific fields and branches, regions, communities, and society, development of strategic and policy documents of the state, and their periodic adjustment. Also, there are no uniform rules regarding the preparation of planning documents for different phases of the national resilience ensuring cycle (primarily ensuring preparedness, response, relief efforts, post-crisis recovery) and inter-agency cooperation to generate joint capabilities, designate the sequence of use of different resources (both governmental and non-governmental), forces and means, including international assistance.

According to the theoretical background, as described in Chapters 1 and 2 of this monograph, world best practices, and also, the specifics of Ukrainian legislation, it is advisable to introduce the strategic planning cycle in Ukraine, encompassing processes with different periodicities assembled on the basis of a common goal. In particular, according to the Law of Ukraine (2018) (Part 1, Article 26), the National Security Strategy is a long-term planning document. The same applies to planning documents in the areas of national security, as specified in this Law. However, the assessment of risks and capabilities (via self-assessment) and testing of approved plans during exercises and training sessions should take place annually to timely adjust the national resilience ensuring benchmarks and priorities, specific and sectoral resilience plans, and emergency and crises related plans. The National Security Strategy's adjustment should be preceded by preparation of a comprehensive report on the results of assessment of risks and capabilities and identification of threats and vulnerabilities in the field of national security of Ukraine.

The above mentioned strategic planning cycle in the field of national security is presented in *Fig.* 5.3. It shows a shorter cycle going from comprehensive risk assessment to adjustment of plans inside a longer national security strategy development and updating cycle.

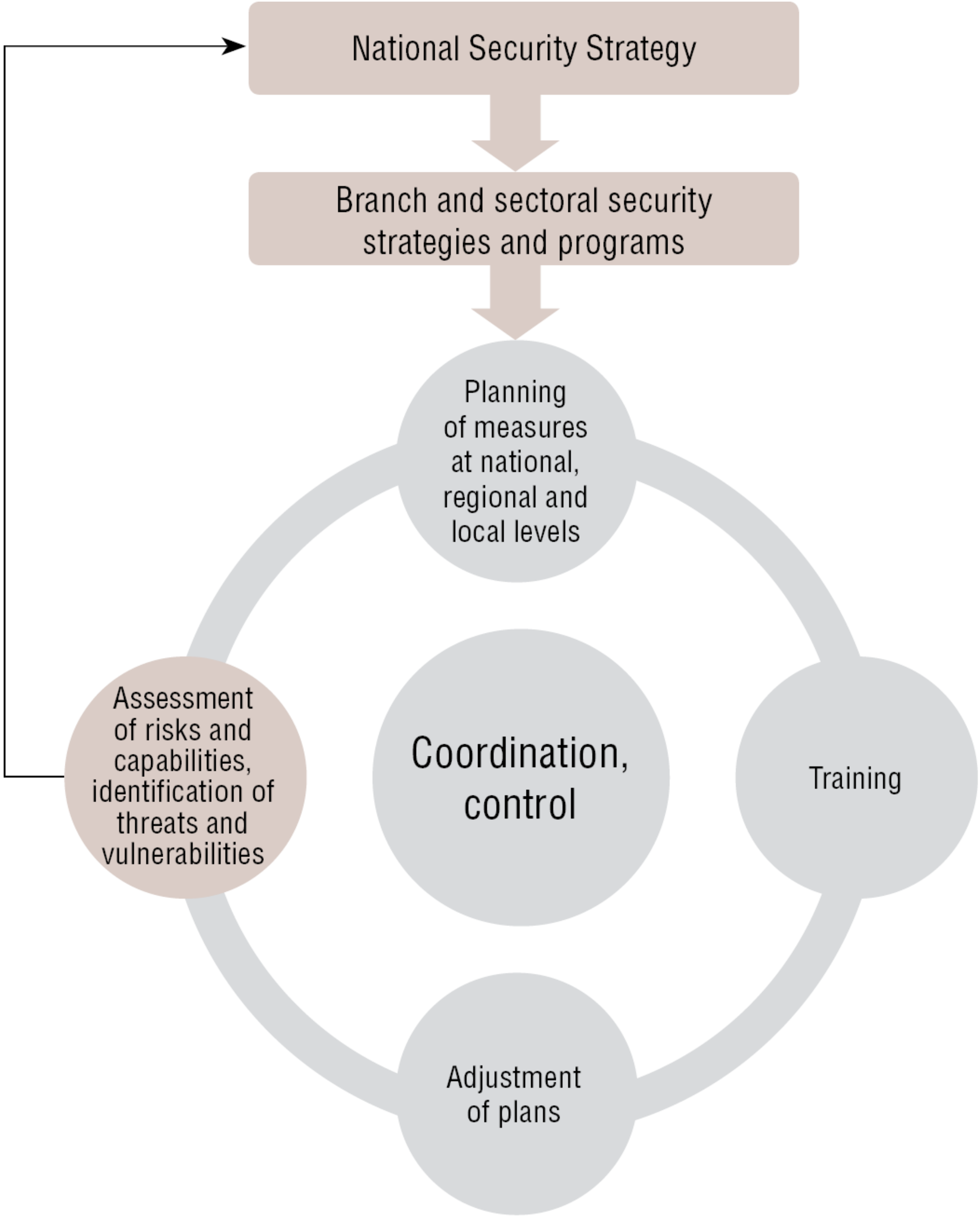

National Security Strategy
Branch and sectoral security strategies and programs
Planning of measures at national, regional and local levels
Coordination, control
Training
Adjustment of plans
Assessment of risks and capabilities, identification of threats and vulnerabilities

Fig. 5.3. **The strategic planning cycle in the field of national security**
Source: developed by the author.

To establish a holistic approach to strategic planning in the state, it is advised to develop and adopt the *law of Ukraine on public strategic planning* to designate the following:

- the types of planning documents in the state:

  - strategic (the National Security Strategy and long-term planning documents in the areas of national security, the Economic, and Social Development Strategy);
  - operational (including plans of response to certain threats and emergencies and universal protocols of concerted actions in the case of crises);
  - tactical (including plans to respond to a current emergency, relief, and recovery plans);

- regulations and schedules for their development, approval, revision, and alignment with the budgeting process;
- spheres of planning;
- regulations concerning the alignment and integration of plans of different levels in different areas;
- requirements to general structure and content of documents;
- requirements for sources and quality of reporting information for planning;
- regulations for cooperation between central and local authorities and the engagement of civil society and businesses in planning processes;
- regulations for control of planning processes and implementation of planning documents.

In addition to strategic planning, planning of response to certain threats, emergencies, and crises is crucial for providing national resilience. A special focus should be on the issues relating to universal protocols of concerted actions for responding to crises. As mentioned in the above chapters of this monograph, different risks may produce similar effects (such as jeopardy to life and health of people, damage to infrastructure, residential buildings, and property). Countering these kinds of threats and relief efforts may follow the same response algorithm. In this regard, for planning purposes, it is advised to identify the key groups of generic threats and universal response efforts (*Table 5.1*).

Table 5.1

Form to identify the key groups of generic threats and universal response efforts

Groups of generic threats	**Groups of generic response efforts**	**Capabilities**	**Requirements**
1. Unavoidable threats: - - -	• Adaptation: - - • Ensuring preparedness: -	•	•
2. Threats, the effects of which can be mitigated: - - -	• Prevention: - - • Prophylaxis - - • Ensuring preparedness: -	•	•
3. Threats requiring active countering: - - -	• Ensuring preparedness: - - • Response - - • Recovery: -	•	•

Source: developed by the author.

National security and resilience ensuring measures can include regulatory, organizational, technical, financial, economic, social, educational, and international ones.

The Law of Ukraine “On National Security of Ukraine” needs to be amended to include an integrated cycle of strategic planning in the field of national security of Ukraine and a requirement to formulate national resilience ensuring goals and objectives in the planning documents at different phases.

It is expedient to launch methodological training in Ukraine at the initial stage of strategic planning documents development in the areas of national security of Ukraine. The leading scientific institutions, including the National Institute for Strategic Studies, should be involved in organization and facilitation of such events. It is important for all actors involved in the development and implementation of planning documents to understand clearly what is required from them and be prepared to implement measures that are set forth in approved documents.

The development of action plans to implement the subject documents with clearly formulated objectives, benchmarks, responsible entities, and guides is an integral part of Ukraine's National Security Strategy implementation process. The outcomes of sectoral security strategies should be evaluated against established criteria and indicators. The state authorities, responsible for the implementation of sectoral strategies, should publish annual progress reports, similarly to what is required for the Strategy of Public Security and Civil Protection of Ukraine in accordance with Part 5, Article 29, the Law of Ukraine "On National Security of Ukraine" (Law of Ukraine, 2018).

Considering the negative experience of implementing the previous versions of the National Security Strategy of Ukraine, the subject Law of Ukraine needs to be amended to include a control and progress reporting procedure for implementation of the Strategy and other planning documents in national security areas.

The clauses of the Law of Ukraine "On National Security of Ukraine" (Law of Ukraine, 2018) regarding a comprehensive review of the security and defense sector of Ukraine and its components also need improvement to incorporate evaluation of capabilities and level of preparedness for threat, emergency, and crisis response, as well as regular self-assessment practices, should be applied across state and local authorities in terms of ensuring resilience to certain threats, emergencies, and crises. The above novelties will foster improved planning effectiveness, correspondence of efforts to existing or anticipated threats and risks, and timely adjustment of plans to accommodate the emerging vulnerabilities.

Also, it would be advisable to incorporate planning norms in the sphere of ensuring preparedness and response to crises into the Law of Ukraine "On National Security of Ukraine" (Law of Ukraine, 2018), to include definition of "crisis" and the main types of crises, that will be subject to planning and implementation of measures to develop preparedness and response, as well as the legal framework for planning in appropriate areas.

The development of action plans in the sphere of civil protection, prevention, and response to certain threats and crises should take into account the goals and objectives referring to the strengthening of national resilience. Such measures are required, in particular, to support:

- regular exercises and training sessions involving communities and the population;
- establishment of strategic communications;
- resilient communications with communities and population;
- engagement of communities, public associations, businesses and other stakeholders in the planning of measures in the sphere of civil protection, prevention, and response to certain threats and crises.

The development of international cooperation is an important area in terms of improving planning in national security and resilience. Thus, within the framework of Ukraine – NATO cooperation, it is expedient to focus, inter alia, on acquiring by the central and local government representatives of appropriate knowledge and skills in the field of planning a response to crises and reviews on preparedness issues, including by joint exercises and training sessions with NATO representatives.

5.7. Multi-Level Comprehensive National Risk Assessment System Creation Perspectives

5.7.1. Prospective Model for Organization of Comprehensive Multi-Level Risks and Threats to National Security Assessment System of Ukraine

General risk assessment and risk management recommendations are provided in ISO standards. In Ukraine, adapted versions of some of these standards, such as DSTU IEC/ISO 31010:2013 are in effect. However, it should be borne in mind that they provide general recommendations and do not exclude further development and refinement of their clauses for different branches.

The establishment of a multi-level comprehensive national risk and threat assessment system in Ukraine should focus on improvement of strategic planning and analysis, enhancement of preparedness of the state and society to respond to the broad spectrum of threats, and national resilience strengthening in general. The establishment of such a system requires legal regulation of fundamental principles of its operation, its inherent processes, approval of uniform procedure and methodology to assess risks and threats to national security and relevant capabilities, designation of organizational model and principles of cooperation between state authorities, scientific institutions, and other actors involved in such activities.

An important objective of the national risk and threat assessment system is to specify generic groups of risks and their consequences for the key target groups, and based on such analysis, develop universal protocols of concerted response to threats and crises at different phases of their deployment. Scenario-based projections and simulation of crises will support timely prioritization and updating of actions plan for specified periods. The uniform methodology of assessment of risks and threats to national security is critically important, as it will enable comparison and prioritization of threats and their consequences in different areas based on uniform principles and criteria.

The subject comprehensive assessment system should extend beyond the mere assessment of risks and threats to national security, and should encompass also evaluation of capabilities that are required to effectively respond to threats at different phases. In view of the features of the administrative and territorial organization of our state, the comprehensive risk and threat assessment system should be multi-level, i.e., function both at national and regional levels. However, it is expedient to introduce different levels of this system in phases in Ukraine.

The *main processes* to be implemented in Ukraine to establish the comprehensive risk and threat assessment system are as follows:

- annual risk and threat assessments, emergency and crisis projection and simulation;
- generation and maintaining national and regional threat registers;
- annual resilience self-assessment to be carried out by state and local authorities, strategic enterprises and organizations;
- analysis of correspondence of existing capabilities to identified threats and scenario-based projections of their occurrence and development of crises, and also identification of vulnerabilities and needs to enhance capabilities. This work should take be done every five years based on the results of the comprehensive and sectoral reviews of the national security and defense sector in Ukraine.

The results of comprehensive assessment of risks and capabilities, identification of threats and vulnerabilities should be taken into account in shaping public policy in national security and resilience, including drafting of a new version of the National Security Strategy of Ukraine or refinement of its clauses.

Recognizing the significance of the above conceptual framework of building national security ensuring system and world best practices, it is expedient to propose the *model of a multi-level comprehensive system of assessment of risks and threats to the national security of Ukraine,* as presented in Fig. 5.4 (Reznikova et al., 2021).

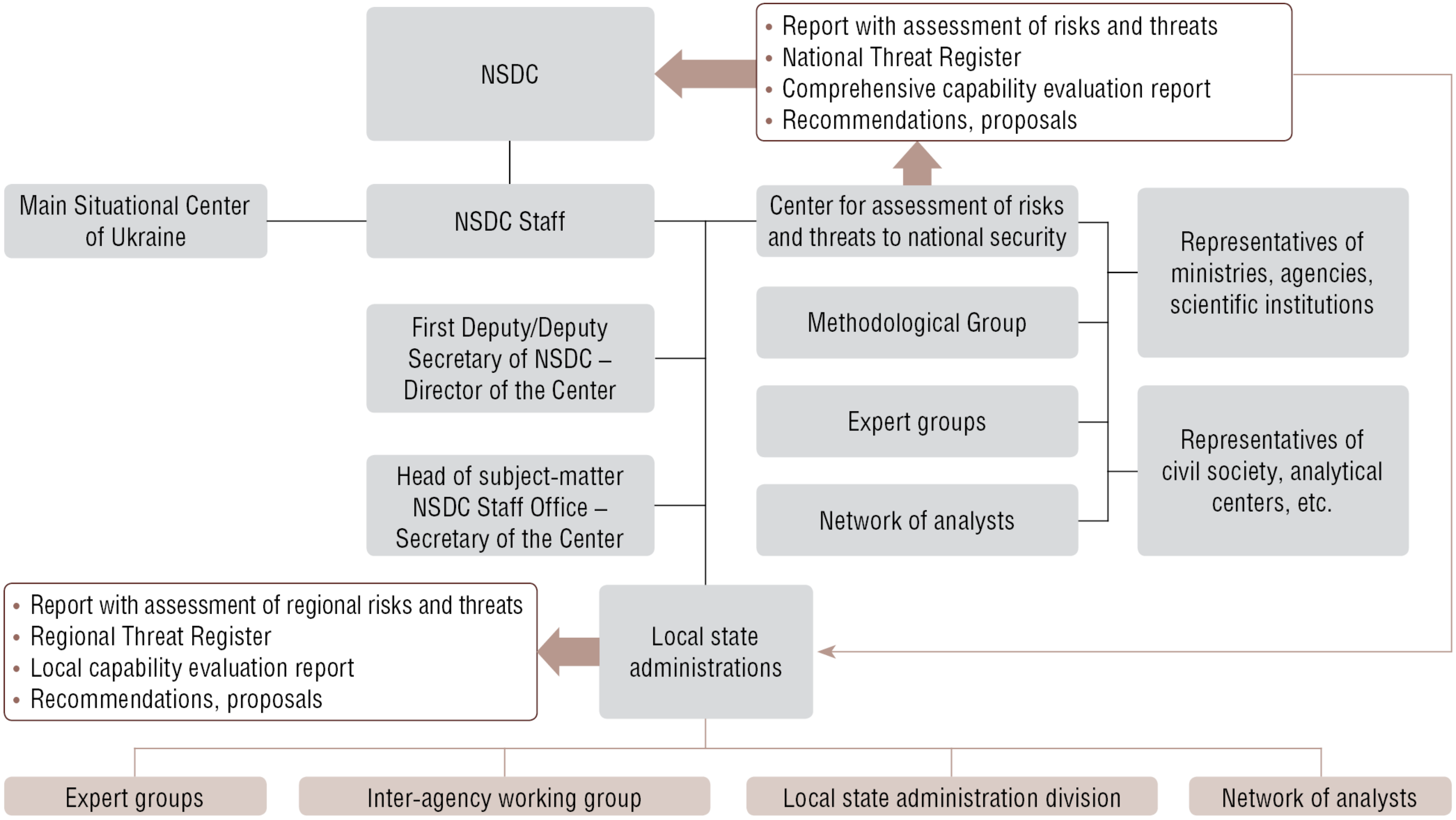

NSDC
Report with assessment of risks and threats
National Threat Register
Comprehensive capability evaluation report
Recommendations, proposals
Main Situational Center of Ukraine
NSDC Staff
Center for assessment of risks and threats to national security
Representatives of ministries, agencies, scientific institutions
First Deputy/Deputy Secretary of NSDC – Director of the Center
Methodological Group
Expert groups
Representatives of civil society, analytical centers, etc.
Head of subject-matter NSDC Staff Office – Secretary of the Center
Network of analysts
Report with assessment of regional risks and threats
Regional Threat Register
Local capability evaluation report
Recommendations, proposals
Local state administrations
Expert groups
Inter-agency working group
Local state administration division
Network of analysts

Fig. 5.4. **The model of multi-level comprehensive system of assessment of risks and threats to the national security of Ukraine**
Source: developed by the author.

The organization of operation of the proposed multi-level comprehensive system of assessment of risks and threats to the national security of Ukraine (*Fig. 5.4*), coordination of efforts of its actors and maintenance of the National Threat Register should be vested in the *Center for assessment of risks and threats to the national security of Ukraine* (hereinafter – the Center), which is expedient to establish as a supplementary working entity of the National Security and Defense Council of Ukraine. Establishment of such centers is quite common practice in the world.

According to Article 14, the Law of Ukraine "On the National Defense and Security Council of Ukraine" (Law of Ukraine, 1998), the inter-agency commissions, working and advisory entities may be established based on the NSDC's decision and funding from the State Budget of Ukraine to elaborate on and complex address issues of inter-sectoral character and provide scientific, analytical and forecasting support to the National Security and Defense Council of Ukraine. The functions and responsibilities of these entities have to be set out in specific regulations that are subject to approval by the President of Ukraine.

According to the subject Law of Ukraine, the key *functions* of the Center, inter alia, should be defined as follows:

- coordination and control of executive authorities and other actors involved in the processes related to the assessment of risks and threats to the national security of Ukraine;
- control of the receipt and processing of necessary information, its storage, confidentiality, and use in the interests of the national security of Ukraine;
- analysis of security environment status and tendencies in its development in Ukraine and across the world;
- projecting crises and threats to the national interests of Ukraine.

The key *areas* of the Center's activities should be as follows:

- organizational and methodological support of assessment of risks and threats to national security, including those of inter-sectoral character;
- ensuring scientific, analytical, and forecasting support of NSDC of Ukraine regarding strategic planning issues in the areas of national security and defense, including within the framework of the cycle of National Security Strategy of Ukraine development and implementation;
- drafting proposals to the President of Ukraine regarding implementation of domestic and foreign policy in the field of national security and resilience, including the definition of strategic national interests of Ukraine; conceptual approaches to national security and resilience and their directions; improvement of national security ensuring system and building defense capacity in the context of addressing objectives relating to the strengthening of national resilience; material, financial, personnel, organizational and other support to eliminate vulnerabilities and develop capabilities in the field national security and resilience;
- implementation of political, social, military, scientific, technical, ecological, information-wise, and other measures in line with the scale of potential and actual threats to the national interests of Ukraine;
- drafting appropriate strategic and program documents, etc.

Considering the principal goals and roles of the Center, its key *task* should include the following:

- strategic analysis of security environment, identification, assessment, and ranking of current and anticipated risks and threats to the national security of Ukraine, identification and assessment of their impacts on different target groups, development of scenarios of risks and threats occurrence and development of crises, identification of generic groups of current and projected risks and threats;
- identification of long-term trends in global and regional security environment and their impact on national security and sustainable development of Ukraine;

- collection and processing of information to assess risks and threats to the national security of Ukraine in support of decision-making processes in the field of national security;
- ensuring coordination of efforts of security and defense sector bodies and other authorities in the sphere of risk and threat assessment;
- methodological support of local authorities concerning the assessment of threats and capabilities;
- preparing annual reports on assessment of current and anticipated risks and threats to the national security of Ukraine, and self-assessment of strategic government institutions, organizations, and enterprises; a complex report concerning the results of assessment of current and anticipated risks and threats to the national security of Ukraine and the status of appropriate capabilities, proposals regarding drafting a new version of the National Security Strategy of Ukraine or refinement of its specific clauses;
- periodic revision of assessments of current and projected risks and threats to the national security of Ukraine and the status of appropriate capabilities;
- visualization of the results of risks and capabilities assessment, identification of threats and vulnerabilities, preparing the threat data sheets (threat passports);
- publication of results of analysis of threats to the national security of Ukraine pertaining to non-classified information, including the National Threat Register;
- study and adoption of world best practices in the areas of risk assessment, identification and ranking of current and anticipated threats to national security, identification and assessment of their consequences, and the development of scenarios of risks and threats occurrence and deployment of crises;
- providing international cooperation regarding the use of advanced methods and technologies in strategic analysis of security environment, risk and threat assessment, projection and simulation of crises.

Based on the results of assessment, *proposals* should be developed concerning:

- priorities in the national interests of Ukraine and in ensuring national security and resilience;
- goals, key areas, and objectives of public policy in national security and resilience;
- areas and objectives of the reform and development of security and defense sector and enhancement of capabilities required to strengthen national resilience;
- resources required to implement the National Security Strategy of Ukraine;
- improvement of conceptual approaches to and directions of ensuring national security of Ukraine, as well as planning in the areas of national security and defense of Ukraine;
- improvement of legislation, including strategies, concepts, government programs, and other strategic documents, which designate the key areas and objectives of public policy in the areas of national security and resilience;
- universal protocols of concerted actions to respond to threats, emergencies, and crises at different phases.

Such proposals should be duly referred to the President of Ukraine and the National Security and Defense Council of Ukraine.

The Center should also be assigned the task of formulation, maintenance, and periodic update of the *National Threat Register* (hereinafter – Register), as a publicly accessible version of the results of assessment of risks and threats to the national security of Ukraine.

The Register should include the following elements:

- overview of security environment of Ukraine;
- description of current and anticipated threats to the national security of Ukraine, the main types of crises to include emergencies that may occur within the next five years and their potential consequences for the people;

- description of legislative mechanisms and procedures for threat, crisis and emergency response, the list of responsible state authorities and their contact information, and crisis management recommendations to population;
- the main provisions of the methodology of risk assessment and threat ranking.

To complete the assigned tasks, the Center should be duly *entitled* to:

• establish a network of analysts in the area of strategic analysis of security environment and assessment of risks and threats by involving representatives of central and local authorities, research institutions, enterprises, non-governmental organizations, and independent experts;

• request from state and local authorities, enterprises, institutions, and organizations and obtain, at no cost, self-assessment reports, statistics, reference, information and other data to address the issues that are within the competence of the Center;

• utilize capabilities of the network of situational centers, including the Main Situational Center of Ukraine;

• use information databases of state authorities, government communication systems, special communication networks, and other technical means;

• organize scientific, research, developmental, and other work in the sphere of strategic security environment analysis;

• initiate conferences, seminars, and meetings on the issues that are within the competence of the Center, with the involvement of representatives of state authorities, national and international organizations, institutions, and experts;

• cooperate, according to the assigned tasks, with state and local authorities, enterprises, institutions, and organizations;

- organize seminars and trainings for representatives of local authorities with regard to the assessment of regional risks and capabilities and the identification of threats and vulnerabilities at local level;
- duly designate the access regime to assessment results.

In view of the complex nature of present-day threats, the Center should apply both traditional and advanced methods and technologies of risk and threat assessment and projection and simulation of emergencies and crises.

In its activities, the Center should be governed by the Constitution and laws of Ukraine, acts of the President of Ukraine, Regulation on the Center, and other regulatory acts of Ukraine. In the *organizational context*, it is expedient to establish the Center based on the principle of departmental representation. The appointment of deputy leaders of ministries, agencies, and scientific institutions as members of the Center will ensure high level representation, as well as reliable inter-agency liaison in the sphere of risk and threat assessment.

The function of risk and threat assessment and identification of threats in different areas would be expedient to assign to the ministries, agencies, and organizations that will engage in the Center's activities either directly via their representatives, who are members of the Center, or on a separate order. At that, the subject ministries, agencies, and organizations can apply specific risk and threat assessment methods within the areas of their responsibility. The uniformity of risk assessment methodology includes harmonization of risk assessment principles and general approaches in different spheres to be able to compare the results. Also, the subject entities should prepare data for comprehensive risk assessment reports in the prescribed form and provide information necessary for the National Threat Register generation and maintenance.

Identification of the *spheres of national security* requiring risk assessment and threat identification, and distribution of responsibilities between the Center and involved ministries and agencies with regard to risk assessment and threat identification, as well as generation of necessary reports and papers, are pivotal provisions of risk assessment and threat identification methodology to be developed by the Center.

Considering the Center's mission and functions in the sphere of elaborating on and comprehensively solving problems of inter-agency nature, scientific, analytical, and forecasting support to the National Security and Defense Council of Ukraine, the establishment and operation of the Center under the National Security and Defense Council of Ukraine (NSDC) would be the most effective solution, which can be implemented at the current moment as follows:

1) establish the Center as NSDC's supplementary working entity; or
2) the Main Situational Center of Ukraine to perform the function of the Center while undergoing comprehensive reform and transformation into NSDC's working entity.

It is expedient to provide the Staff of the NSDC with information analysis, experts, organization, logistics, and other types of support for the Center. In the future, it is advisable to establish a separate organizational structure within the NSDC, which will combine the Center for National Security Risks and Threats Assessment, the Main Situational Center of Ukraine, the Center for the Critical Infrastructure Resilience, and other similar organizations that were established within the NSDC and focus on enhancing the national resilience. Such an organization shall involve leading experts in the fields of strategic analysis and threat assessment. This approach will allow combining technical and analytical components within a strategic analysis and planning system.

In case the Main Situational Center of Ukraine will be charged with fulfilling the functions of the Center for National Security Risks and Threats Assessment, it should be transformed into a working body of the NSDC. Its technical capabilities need supplementing with an analytical component that will identify the main tasks to work upon within the existing hardware and software package as well as its further development areas.

The proposed Center for National Security Risks and Threats Assessment needs to have a structure, which includes its head, secretary, and other members of the Center, as well as a Methodology group.

It is expedient to determine the members of the Center by positions at the level of authorized deputy heads of executive bodies, state institutions, and scientific organizations. This refers in particular to the Ministry of Defence, Ministry of Internal Affairs, Security Service of Ukraine, Foreign Intelligence Service, Defence Intelligence of the Ministry of Defence, State Service of Special Communication and Information Protection of Ukraine, State Migration Service, State Financial Monitoring Service, Ministry of Economy, Ministry of Agrarian Policy and Food, Ministry for Strategic Industries, Ministry of Environmental Protection and Natural Resources, Ministry of Energy, Ministry of Infrastructure, Ministry of Health, Ministry for Communities and Territories Development, Ministry of Finance, National Bank of Ukraine, as well as the National Institute for Strategic Studies, the Institute for Economics and Forecasting of the National Academy of Sciences of Ukraine, the National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute." This list may include other governmental agencies and scientific organizations as well.

Since authorized state bodies will be entrusted with assessing risks and threats, it is logical to assume that members of the Center as senior executives within these bodies, on the one hand, shall provide for a representation of respective bodies within the Center, and on the other hand – control of fulfillment of assigned tasks related to assessing risks, threats, and producing respective results.

In addition, to perform assigned tasks, the Center shall have the right to shape the network of analysts in the fields of security environment strategic analysis and risks and threats assessment, targeted working group and expert level teams, as well as arrange for meetings and other communication events.

It is expedient to appoint as the *head of the Center* the First Deputy (or Deputy) Secretary of the National Security and Defense Council of Ukraine, who is responsible for ensuring national resilience. Due to the Regulation on the Commission for the Coordination of Euro-Atlantic Integration of Ukraine, as approved by the President of Ukraine (2019d), the Vice Secretary or one of the deputies of the Secretary of the NSDC of Ukraine, whose scope of duties includes the issues of developing the national resilience system, is considered to be the National Coordinator for the Ukraine-NATO cooperation in the area of building the national resilience. Thus, it is expedient to combine the functions of a national coordinator and the head of the Center.

The following responsibilities may be assigned to the head of the Center:

- managing the Center's operations, identifying its operating procedures, convening and chairing meetings of the Center;
- approving the following:

- composition of working and expert teams as they get established;

- methodology for conducting an assessment of risks to the national security of Ukraine and their consequences, ranking and defining priority of threats, and developing projected scenario of the threats and crises development;

- methodology for evaluating capabilities in the areas of preventing threats and crises, providing for readiness and response to them, minimizing and eliminating their consequences based on the outcomes of a comprehensive review of the security and defense sector and sectoral reviews;

- a draft annual report on the results of the assessment of current and projected risks and threats to the national security of Ukraine;

- a draft comprehensive report on the results of the assessment of current and projected risks and threats to the national security of Ukraine as well as the status of corresponding capabilities following the discussion of the report at the Center's meeting;

- structure, format, and procedures for maintaining the National Threat Register;

- structure and form of the reports on assessment outcomes that are drafted by the Center.

In addition, the head of the Center shall:

- assign tasks to the members of the Center to draft annual and comprehensive reports on the results of assessing current and projected risks and threats to the national security of Ukraine, as well as the status of respective capabilities; monitor the tasks performance;
- make decisions on releasing the results of the national risks and threats assessment as related to non-classified information;
- represent the Center in its relations with state agencies, enterprises, and international and public organizations.

In accordance with the above proposals on the legal basis for the establishment of the Center, its head should be appointed and dismissed by the President of Ukraine.

It is expedient to assign as the *Secretary of the Center* the head of a structural division of the Staff of the National Security and Defense Council of Ukraine, which is responsible for the issues of strategic planning, analysis, and national resilience. The relevant structural division of the NSDC’s Staff shall support the activities of the Center on the organizational level, but also possess a proper professional potential to carry out appropriate analytical work in the field of strategic analysis and, in particular, assess risks and threats.

It is advisable to assign broad responsibilities to the Secretary of the Center to include support of the following:

- accumulation, consolidation, and processing of information received from members of the Center, other ministries, departments, institutions, enterprises, and organizations required to assess current and projected risks and threats to the national security of Ukraine and the state of relevant capabilities, using the capabilities of the Main Situational Center of Ukraine as well as the preparation of annual and comprehensive reports;
- consolidation of proposals in order to draft protocols of concerted actions to respond to threats and crises, including emergencies, at different stages of their development;

- maintenance and periodic update of the National Threat Register.

Based on the established procedures the Secretary of the Center also shall: draft and submit to the head of the Center proposals for the Center's working plans; draft meeting agendas taking into account proposals from Center members; establish working and expert teams and composition of such teams; conduct communication events; coordinate the work of established working and expert groups; support the development and submission to the head of the Center as well as support discussion at the Center's meeting of draft annual reports on results of assessing current and projected risks and threats to the national security of Ukraine; create a comprehensive report on results of assessing current and projected risks and threats to the national security of Ukraine as well as the status of respective capabilities; inform the head of the Center on the status of implementing the decisions made by the Center; submit proposals to the head of the Center on improving the Center's operations; and perform other tasks as assigned by the head of the Center.

The responsibilities of the *members of the Center* shall primarily cover the issues of supporting the following according to the established methodology for their field of responsibility:

- assessment of risks and threats to the national security of Ukraine and their consequences in terms of defined target groups;
- development of scenarios for the implementation of risks and threats and the development of responses to a crisis;
- identification of long-term trends in global and regional security environments, assessing their influence on national security and the sustainable development of Ukraine;
- evaluation of correspondence between existing capabilities and identified risks and threats as well as scenario forecasts for their implementation and development of crises, identification of vulnerabilities, and the need to enhance capabilities;

- drafting the proposals to shape protocols of concerted actions aimed at responding to threats and crises, including emergencies in various stages of their development;

If necessary, the members of the Center can initiate the following:

- receiving statistics, analysis, and other types of information from ministries, departments, institutions, organizations, and enterprises. This information is necessary to evaluate risks and threats to the national security of Ukraine and the status of its respective capabilities;
- establishment of working and expert groups in the area of their activities;
- conducting communication events.

It is also advisable to commit the members of the Center to provide, following identified procedures and within specified timeframes (to include remotely) in compliance with legislative requirements in securing classified information:

- data and information necessary to shape and update the National Threat Register;
- results of assessing the risks and threats to the national security of Ukraine.

A fundamentally important issue in the work of the Center is the development of methods and approval of a single evaluation methodology. To this end, it is expedient to form *a Methodological Group* within the Center. Its responsibilities shall include:

- development of a unified comprehensive methodology of evaluating risks and threats to the national security of Ukraine as well as their consequences, ranking and identifying priorities of threats, drafting scenarios of manifestation of threats, and development of crises;
- development of a unified comprehensive methodology of evaluating capabilities in the areas of preventing threats and crises, providing for the readiness and response to them, minimizing and eliminating their

consequences based on the outcomes of a comprehensive security and defense sector review as well as sectoral reviews;

- monitoring compliance with approved methods by all state and local authorities as well as institutions, organizations, and experts involved in assessment;
- examination of the draft annual report on the results of assessing current and projected risks and threats to Ukraine's national security and a comprehensive report on the results of assessing current and projected risks and threats to Ukraine's national security and the state of relevant capabilities concerning their completeness, reliability, and compliance with a certain methodology;
- identification of the structure, format, and contents of the National Threat Register;
- identification of the structure and format of the assessment reports drafted by the Center;
- amending and supplementing approved methodologies, if necessary.

Taking into account peculiarities of operations as well as the high scientific and analytical potential of organizations, it is expedient to supplement the Methodology group with respective experts from the National Institute for Strategic Studies, the Institute for Economics and Forecasting of the National Academy of Sciences of Ukraine, the National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute," as well as other leading scientific organizations of Ukraine, if required.

According to established practice, members of the Methodology Group and organizations headed by them should not be directly involved in assessing risks and threats to the national security of Ukraine and the state of relevant capabilities. This approach is aimed to provide impartiality during the examination of the obtained results and the draft reports. The establishment and functioning of the Methodological Group with appropriate responsibility will ensure a necessary balance between the results of scientific research and the pragmatic goals of public administration.

It is expedient to determine the main form of work of the Center as meetings that are chaired by the head of the Center. These meetings shall be conducted when necessary but no less than once a quarter. It should be established that the meeting of the Center is valid if it is attended by more than half of its members. The decision of the Center should be taken at the meeting by a majority vote of its members. In the case of an equal distribution of votes, the vote of the chairman of the meeting should be decisive. If a member of the Center does not agree with the decision, he/she should have the right to express a separate opinion in writing, and this opinion will be attached to the meeting minutes. The decisions made by the Center should be recorded in the protocol signed by the chairman of the meeting and the secretary of the Center.

It is expedient to determine the decisions of the Center as mandatory for consideration by state and local authorities, military formations established by the laws of Ukraine, enterprises, institutions, and organizations.

The procedure for the functioning of the Center, its responsibilities, involvement of scientific institutions, non-governmental organizations, independent domestic or foreign experts, the mode of access to the results of its work, and other issues should be determined by the *Regulation on the Center*, which should be approved by the President of Ukraine due to the Article 14 of the Law of Ukraine “On the National Defense and Security Council of Ukraine” (Law of Ukraine, 1998). To ensure the continuity of the Center’s operations, it is necessary to determine its official composition in the Regulations, and the NSDC Secretary shall be assigned to approve its membership.

Since the process of building a national resilience ensuring system in Ukraine has not yet gained sufficient momentum, the introduction of a multi-level system for assessing threats in the field of national security should be carried out in several stages.

Short-term (priority) tasks (1-2 years) should include the development and adoption of legal acts on the establishment and functioning of a national system of risks and threats assessment, as well as the designation (or formation) of a body responsible for coordinating relevant activities.

Taking this into account, during *phase one* of establishing the mentioned above national system it is expedient to introduce the following processes:

- annual assessment of risks and threats to Ukraine's national security as an element of strategic planning and adaptive management.
- development of annual reports on the results of the assessment of risks and threats to the national security of Ukraine.
- assessment of capabilities to counter current and projected threats to national security and crises, including emergencies, based on the results of a comprehensive review of the security and defense sector of Ukraine and sectoral reviews.
- drafting periodic (every five years) comprehensive reports on the results of assessing current and projected risks and threats to Ukraine's national security and the state of relevant capabilities as the basis for the development of the draft National Security Strategy of Ukraine.

Also, at this stage, it is necessary to decide on the establishment (or performance of its functions) of the Center for national security risks and threats assessment in Ukraine, which will provide the functioning of a relevant system at the strategic level and to develop a methodology for assessing risks and threats to national security and the state of relevant capabilities.

Mid-term tasks (3-5 years) include expanding the national risk and threat assessment system to regional and local levels.

Accordingly, in *phase two* of the mentioned national system building it is expedient to:

- identify local authorities whose responsibilities will include coordination of actions in the field of assessing regional risks and threats, as well as creating and maintaining appropriate registries;

- establish regional formats (structures) of interagency cooperation in ensuring the security of regions. These structures will operate permanently, and their responsibilities will include, in particular, shaping regional threat registries;
- introduce a unified methodology for assessing risks and threats to national security and the state of relevant capabilities at all levels in the state;
- develop and implement training programs for identifying threats and vulnerabilities, assessing risks and capabilities;
- establish interaction and exchange of information between the actors of assessment of the national security risks and the state of relevant capabilities at the national, regional, and local levels;
- the Center for national security risks and threat assessment of Ukraine shall arrange and conduct training for regional representatives on methodology and processes of risk and threat assessment, as well as establish reliable communications with local administrations and established structures for interagency cooperation.

In *phase three* of the building national system for assessing risks and threats, it is necessary to introduce the following:

- drafting periodic regional reports on results of assessing risks and threats;
- regional threat registries.

It is expedient to approve the decision of the National Defense and Security Council of Ukraine on implementing phase one of building the multi-level risk and threat assessment system in the national security area as well as functioning the Center for national security risks and threats assessment in Ukraine. Due to Article 10 of the Law of Ukraine “On the National Defense and Security Council of Ukraine,” the decisions are put into effect by decrees of the President of Ukraine and are mandatory for execution by state and local authorities (Law of Ukraine, 1998).

Following that, according to Part two of Article 14 of this Law, the Regulation on the Center for assessing risks and threats to the national security of

Ukraine should be approved by a decree of the President of Ukraine. The development of draft decrees of the President of Ukraine on the establishment of the mentioned Center should take into account the requirements of the Decree, adopted by the President of Ukraine (2006).

Therefore, taking into account the above listed conceptual approaches to the establishment and introduction in Ukraine of a multi-level comprehensive system for assessing risks and threats in the field of national security and the peculiarities of legal regulation of the relevant sphere, it is expedient to develop such draft regulatory and legal acts:

an NSDC decision, which includes the following:

- conducting an annual assessment of risks and threats to the national security of Ukraine on a permanent basis as a part of strategic planning and adaptive management;
- establishing annual reports on results of assessing risks and threats to the national security of Ukraine;
- assessing capabilities to counteract current and projected risks and threats to the national security based on the comprehensive review of the security and defense sector of Ukraine and appropriate sectoral reviews;
- establishing periodic (once every five years) comprehensive reports on the results of evaluating current and projected risks and threats to Ukraine’s national security as well as the status of relevant capabilities as the basis for developing the draft National Security Strategy of Ukraine;
- establishing the Center for national security risks and threats assessment of Ukraine as an NSDC supplementary working body or delegating its functions to the Main Situational Center of Ukraine through its transforming into an NSDC working body.

Decree of the President of Ukraine enacting the mentioned decision of the NSDC of Ukraine.

Decree of the President of Ukraine on approving the Regulation on the Center for national security risks and threats assessment of Ukraine and assigning its head.

Adopting and implementing the mentioned regulatory and legislative acts will facilitate the development of a strategic analysis and planning system, enhance the readiness of state and local authorities, and population to respond to crises on various levels of their development, and in general – enhance the national resilience.

5.7.2. Peculiarities of Self-Assessing the Resilience by Government and Local Authorities

An important element of a comprehensive multi-level system for assessing risks and threats in Ukraine should be *self-assessment of resilience*, which should be carried out by ministries, agencies, authorized government institutions, and local authorities within their spheres of responsibility. The purpose of applying such practices is to identify risks and vulnerabilities in the main areas of ensuring national security as well as the organizational resilience of relevant institutions and enterprises of strategic importance and to take timely measures.

Based on the analysis of the best world practices in the field of national resilience and crisis management as well as taking into account recommendations on these issues developed by the UN, OECD, NATO, and other leading international organizations, a general *algorithm* for conducting resilience self-assessment in various fields and areas with relevant recommendations are proposed.

Security Situation Analysis (input data):

- comparison of the main security status indicators within the area of activities with their critical values;
- identification of the generic context of a situation;
- identification of dangerous trends including long-term ones;
- identification of threats to include their manifestations, consequences, and effect on a sector, individual target groups, and other areas;

- identification of factors of negative influence on the sector, which strengthen the impact of an identified threat.

To assess the consequences of the threat influence, it is recommended to take into account the following *key groups*:

- physical facilities (housing, administrative buildings, networks, etc.);
- human capital (life, health, well-being of the population);
- economic and financial resources;
- environment (natural resources, environmental situation, etc.);
- social and political capital (formal and informal social relationships and networks, management systems, political institutions, peace, security, etc.).

Based on the requirements of a specific sector or branch *special target groups* may be separated (e.g., children, working-age people, retirees, and others).

It is recommended to identify target groups that may be most adversely affected by the threat, as well as those that possess substantial resilience potential and are capable of independently counteracting the threat with acceptable losses of functionality. This will contribute to a more objective definition of priorities in shaping the measures to ensure safety, security, and resilience in a relevant branch or area of responsibility.

To assess the risks and analyze the threats in the branch (area of responsibility) it is recommended to use the following *main groups of indicators*:

- indicators of the state of security in a given area;
- probability of a threat or a crisis occurrence;
- scale and severity of the possible consequences of the implementation of a threat or a crisis.

Capability Analysis

The ability of state institutions, systems, and organizations to respond effectively to the development of the crisis or threat implementation during the following *stages* is assessed.

Ensuring readiness. It is recommended to use the following *key assessment* *criteria*:

- reliability (availability of necessary resources, adequacy of the settlement of legal and organizational aspects of activities, dissemination of necessary knowledge and skills among the subjects of response, conducting training, and taking measures to prevent the threat);
- availability of reserves (of all types of resources taking into account branch peculiarities and reserve accumulation standards);
- adaptability (availability of alternative supply sources to provide critical functions of the state, forecasts on options for the threat and crisis development, alternative plans for responding to them, flexibility and effectiveness of management systems, including crisis management).

To ensure *continuity of critical functions of the state, it is recommended to assess*: the availability of alternative sources to provide the population with potable water, food, electricity, alternative sources of electricity and drinking water for administrative buildings; alternative premises where state institutions, strategic enterprises, and their employees, as well as temporarily displaced citizens, medical facilities, and victims, can be temporarily relocated; reliability of cyber protection and communication systems; security of data storage and transmission systems, conditions for working remotely to include the need to protect restricted access information; and alternative transportation routes.

Response. It is recommended to assess: the existence of protocols of concerted actions in a crisis which include common response procedures for typical groups of manifestations of threats and crises and their consequences, the possibility of rapid use of additional (reserve) resources; the existence of a clear distribution of responsibility, procedures for coordinating activities in a certain field; the effectiveness of interagency interaction, crisis management, etc.

Recovery. It is recommended to develop in advance: forecasts and possible scenarios for the development of a crisis as well as follow on recovery based on the time criteria; and the acceptable level of losses in terms of the main target groups (by certain area security indicators and other indicators).

Identification of vulnerabilities

Comparison of threat assessments and the state of relevant capabilities assessments makes it possible to identify branch or area vulnerabilities to certain types of threats. It is expedient to analyze vulnerabilities, first of all, in terms of the main target groups identified for the branch or area.

Using received information (output data)

The results of self-assessment make it possible to draft or clarify *action plans to ensure the security and resilience* of a branch or area of activity and its strategically important facilities including the elimination of identified vulnerabilities and capability building as well as adjusting *strategic development benchmarks*. Particular attention is paid to ensuring effective interagency cooperation, a high level of public confidence in the actions of the state and local authorities, reliable bilateral channels of communication between the state and the population, as well as the continuity of critical services provided to the population and strategically important business.

Schematically, the algorithm for resilience self-assessment in various branches and areas of activity is presented in *Fig. 5.5*.

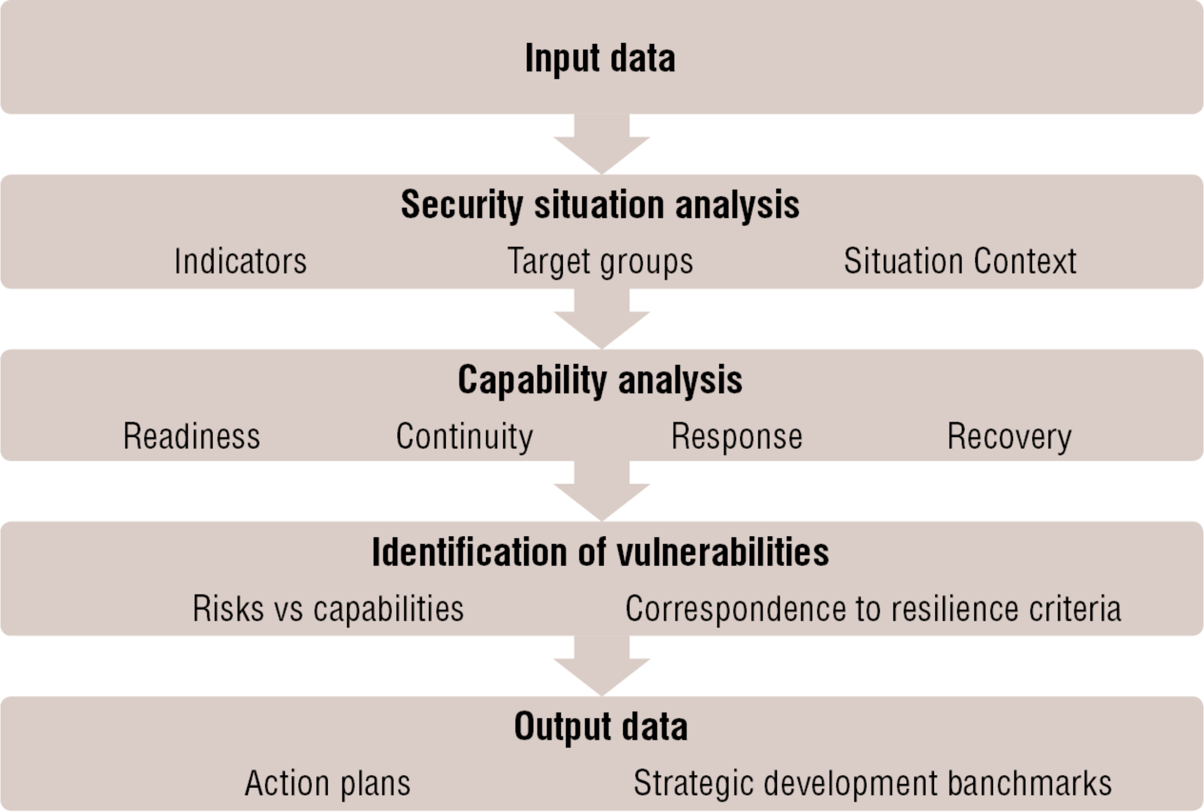


Fig. 5.5. Resilience self-assessment algorithm in various branches and areas of activity.
Source: developed by the author.

To conduct a self-assessment, state and local authorities may be offered a *questionnaire* to fill out with a list of recommended questions (*Annex 3*). The procedure for access to the information contained in answers to questions should be determined by the leadership of the ministry (agency) based on the legislation of Ukraine. The list of questions proposed in the questionnaire can be applied to various branches and areas of activity. However, it should be noted that the resilience assessment of society, communities, critical infrastructure, organizations, and businesses has certain peculiarities. Accordingly, in order to conduct self-assessment in these cases, it is expedient to draft separate lists of questions. In particular, recommendations for assessing the resilience of local communities will be provided in the next subsection of the monograph.

The proposed resilience self-assessment algorithm begins with the analysis of input data, which in the context of a crisis may not be the same for different branches. Thus, in the context of the COVID-19 pandemic, the initial data for the analysis of the biosafety area were dangerous disease spread indicators, and for the economy – the restrictive measures and their consequences for the economy and society. At the same time, typical measures shaping the basis of universal protocols of actions for a crisis in the area of biosafety are those used to prevent the spread of dangerous diseases regardless of their type, and in the economy – those that should be used regardless of the reasons for interrupting business processes (restrictive quarantine measures, disasters, hostilities, etc.)

It is expedient to use the resilience self-assessment algorithm described above during periodic resilience reviews by state and local authorities per the tasks defined within the framework of a comprehensive national system for assessing risks and threats to the national security of Ukraine. The information received should be summarized and analyzed by authorized bodies of the

Secretariat of the Cabinet of Ministers of Ukraine and the NSDC of Ukraine, in particular, the Center for national security risks and threats assessment of Ukraine, in order to develop an appropriate national policy and to rapidly make decisions. It should be added that periodic self-assessment performed by ministries and agencies according to the proposed algorithm cannot replace a multi-level comprehensive system for assessing national security risks and threats, since it is only one of its elements.

5.5 Ways to Provide for the Resilience of Regions and Territorial Communities

5.5.1. Introduction of a Potential Model for Organizational Support to Security and Resilience of Regions and Territorial Communities

Given the fact that Ukraine is a country with significant territory and a multi-level administrative and territorial structure, the development of the resilience capacity of local communities and regions is extremely important in a changing security environment. Based on the results of the analysis of the current situation in Ukraine in this area, it can be determined that the actual tasks are to create legal grounds and favorable conditions for the formation and development of organizational, security, social, and other local capacities, the introduction of effective mechanisms for interaction between state and local authorities, public organizations, private business, and international partners, etc.

In its turn, this requires improving coordination and interagency cooperation on regional and local levels, which should take into account the principles defined by the Concept of Support of the National Resilience System (President of Ukraine, 2021g). The extension of a relevant system to the regional and local level, in particular, provides for the clarification of the authorities of its subjects, a certain redistribution of responsibilities including the transfer of certain national security functions to the local levels, establishment of partnerships with business, and the population. The implementation of this approach will provide for greater system flexibility and efficiency, primarily in responding to unexpected and unconventional threats the response to which requires concerted actions of all actors (Reznikova et al., 2021).

According to essential characteristics of the national resilience concept, the main principles of organizing activities in the field of ensuring the resilience of regions and local communities should be determined as follows:

- lawfulness and continuity, which means ensuring an ability to make, explain and implement decisions even during a crisis in a legal, effective and accountable way at any time;
- clear delineation of responsibilities between the state and local authorities while responding to threats and crises of specified scale, origin, and character;
- interaction and cooperation that provides for regular interagency meetings involving representatives from regional executive bodies, local authorities, civil society, business, and mass media;
- responsibility of resilience ensuring actors for their readiness to respond to threats and crises;
- clarity and appropriate transparency of activities in the area of ensuring resilience of regions and local communities.

Today, Ukraine has created some mechanisms for interagency cooperation at the local level in the areas of countering emergencies and terrorism as well as during the legal regimes of state of emergency and wartime. At the same time, to develop a multi-level comprehensive system for ensuring national resilience, this model of interagency interaction and coordination of activities, aimed at strengthening the resilience of regions and local communities, needs to be improved. First of all, such coordinated activities should provide continuity of management and supply of critical services to the population within a region or a local community in peacetime, during the crises or threats of any origin occurrence as well as during the recovery in a post-crisis period. Among other things, this requires defining a clear scheme for the distribution of authority, streamlining the interaction of various national systems and formats based on the interagency cooperation that functions in the field of responding to various threats and emergencies at the territorial level, implementing protocols of concerted actions, primarily regarding threats and emergencies that are most characteristic for the region. At the same time, it is necessary to ensure an integrated approach to the organization of relevant activities within the framework of a full cycle of ensuring national resilience (monitoring the situation, assessing risks, identifying vulnerabilities, ensuring readiness, planning, preventing, responding, and executing post-crisis recovery).

Taking into account the practice of regional and local level interagency cooperation in the security area in Ukraine as well as world practices, the following main recommendations can be offered for shaping a comprehensive organizational model for ensuring the resilience of regions and local communities:

1. *It is expedient to charge regional state administrations with the lead consolidating role in ensuring regional resilience*. These administrations currently have a lot of power in the area of coordination and ensuring readiness and response to various threats and emergencies. It is expedient to expand their functions to provide coordination of not only territorial subdivisions of central executive bodies, local self-government bodies, enterprises, and organizations, but also the activities of national systems regarding their operations within a relevant administrative-territorial unit.

Besides, the main tasks of regional state administrations in ensuring the regional resilience should include:

- coordination and streamlining activities of various organizational formats (structures) of interagency cooperation that operate within this region;
- establishment of a single secure system for the exchange of information between actors that perform important functions supporting the security and resilience of regions and territorial communities;
- maintaining a regional register of risks and threats;
- facilitating the establishment and introduction of early threat identification and warning systems in the regions;

- controlling the state of readiness of resilience ensuring actors, national systems, and local communities respond to threats and crises within their mandate and their territory;
- coordinating regional, social, and economic development plans with plans for security, resilience, and relevant capability development;
- facilitating interagency exercises and training sessions in the region;
- development of public-private partnership in the area of providing for security and resilience of regions and local communities, interaction with population, and civil society organizations;
- facilitating bilateral communication channels with the population regarding readiness and response to threats and crises;
- promoting the introduction of new technologies in the field of analysis of regional security environment, projecting risks, threat detection, and crisis management.

It is also necessary to identify a clear mechanism for interaction between regional state administrations and the Cabinet of Ministers of Ukraine, National Defense and Security Council of Ukraine, or special bodies established by them in the field of national security and resilience.

2. *The functions, tasks, and composition of local commissions on technogenic and environmental safety and emergencies should also be expanded, transforming them into local commissions for ensuring the security and resilience of regions and local communities.* They should become the main permanent format of interagency cooperation in a relevant field. As part of its functioning, information exchange and coordination of activities for comprehensive risk assessment, threat identification, vulnerability detection, readiness to respond to a wide range of threats, planning of appropriate concerted measures, and post-crisis recovery in the regions should be provided.

It is expedient to involve representatives of not only territorial subdivisions of central executive bodies, local executive authorities, local self-government bodies, enterprises, institutions, and organizations located on the territory of a relevant administrative-territorial unit but also representatives of territorial bodies of the Security Service of Ukraine [SSU], Armed Forces of Ukraine and other military formations to participate in such commissions on a permanent basis. Taking into account the specifics of the issues submitted for consideration, meetings of local commissions on man-made accidents, environmental safety, and emergencies may be with restricted access or open.

An important area of work of commissions should be providing cooperation with other structures of interagency interaction that function or can be established in the relevant territory. In particular, we are talking about the coordination groups of the Anti-Terrorist Center under the regional SSU offices, the main actors of the national cybersecurity system of Ukraine, defense capability ensuring system of Ukraine (including headquarters of the zones and areas of territorial defense), emergency medical services systems, other interagency commissions and working groups that are established locally.

3. *To discuss and coordinate draft managerial decisions as well as solve other common tasks of ensuring security and resilience of regions and local communities, it is expedient to form a network of subsidiary bodies* consisting of interagency working groups, commissions, regional development agencies, and non-government organizations.

Specialized interagency working groups and temporary control commissions can be established under local state administrations or their structural subdivisions and executive committees created from local authorities to monitor the state of readiness, consistency of plans for security and development of regions and local communities, key institutions, organizations, enterprises. To provide for a comprehensive assessment of risks and capabilities, identify threats and vulnerabilities for the region as well as form and maintain a regional register of risks and threats, it is expedient to establish *an interagency working group on risk assessment* and *an interagency coordination group on security planning and resilience*. It is logical to assume that their organizational support should be carried out by an authorized structural division within regional state administrations.

It is expedient to form a network of subsidiary bodies from among experienced experts in the fields and sectors of national security, regional and local development, and public activists. United in a common platform, these advisory and control bodies will provide for comprehensive expert, analytical, and informational support to coordination bodies on security, resilience, and development of regions and territorial communities. Regional development agencies and NGOs can contribute to the creation of common capabilities of local communities and regions to ensure their security and resilience.

All supplementary bodies, joined together in an appropriate network, must function together, in a single algorithm of actions, and perform tasks within the framework of certain work programs and technical tasks. Their common tasks should be determined by the following:

- ensuring whole-of-society cooperation in the field of regional development policy shaping and implementation, ensuring security and resilience of regions and local communities as an integral part of the relevant state policy;
- facilitating the work of coordinating with executive bodies within a relevant administrative-territorial unit, in particular, to ensure readiness, prevent threats of various origins, interact with populations, business, and media as well as neighboring regions and territorial communities on issues of ensuring resilience, development of territorial infrastructure, organization of appropriate scientific and methodological work, and technical consultations;
- promoting the implementation of the principles of adaptive management on the regional, local, and community level.

It is also expedient to apply the practice of creating a *network of scientific, analytical, educational, and methodological centers for the development of resilience of regions and local communities*. Such a network can be organized based on existing private and state think tanks, specialized scientific institutions and universities as well as educational and methodological centers for civil protection and safety of life. The following should be determined as key tasks of the centers for the development of resilience of regions and local communities: the systematization of scientific and practical experience in various areas of security and resilience; joint interdisciplinary scientific research on ensuring the resilience of regions and local communities as well as certain branches; independent examination of draft decisions of authorized territorial executive authorities and local authorities; development of concerted actions protocols, instructions, methods, reference books, guidance in the field of development of resilience of regions and local communities as well as recommendations for establishing interagency interaction between different actors in daily activities and crises.

4. *At the level of local communities, the main role in coordinating support for their resilience building should be assigned to local self-government bodies and their executive committees. Regarding interagency cooperation, commissions should be established and charged with ensuring the safety and resilience of local communities.*

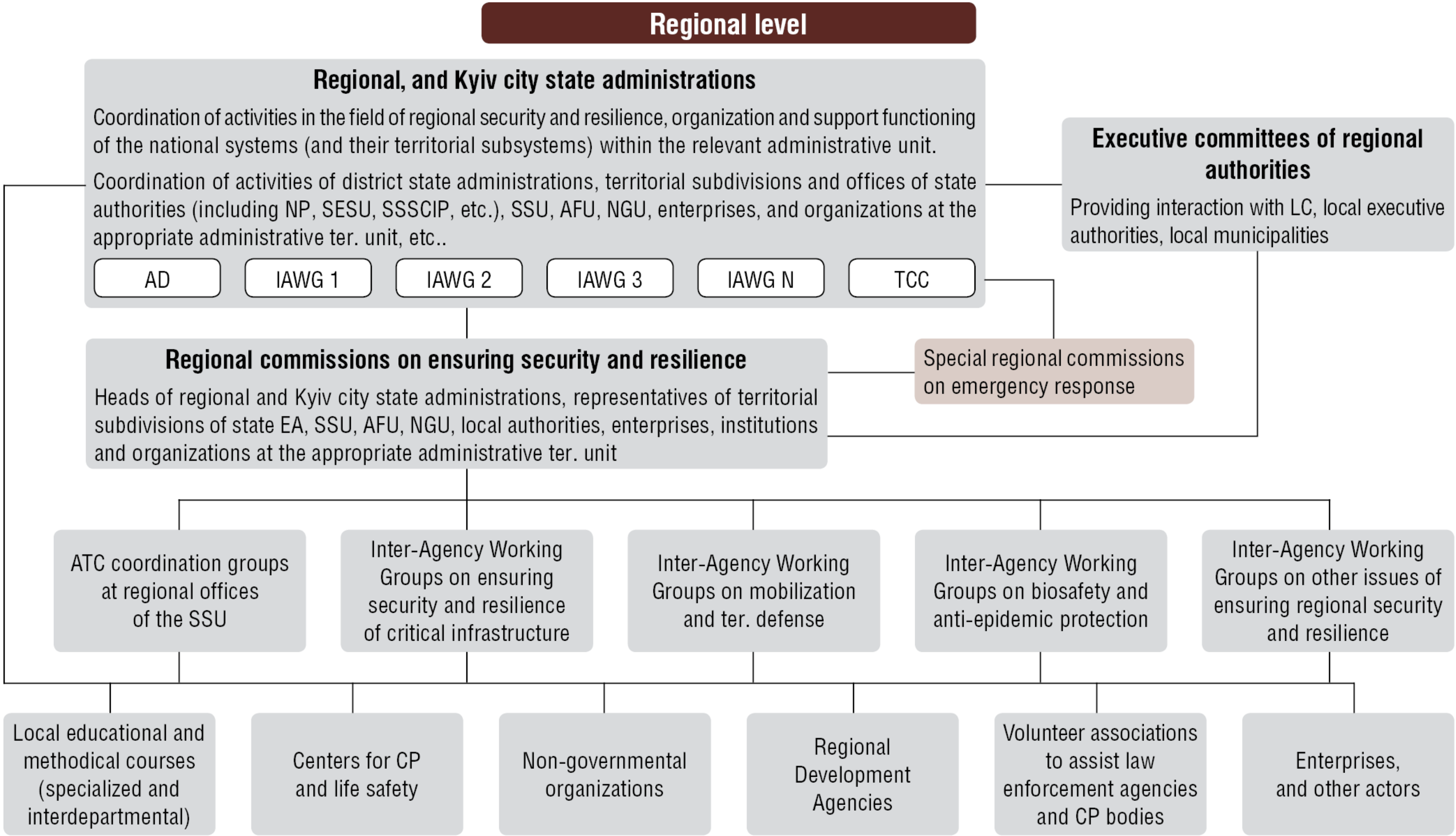
In the context of ensuring the resilience of local communities, the creation of reliable system ties should take place at the horizontal and vertical levels. Taking into account relevant strategic and programmatic national documents and regional development plans, the communities should determine the goals and objectives in the area of providing their resilience as well as their plans to enhance the resilience. There is also a need to periodically assess the progress of their implementation taking into account the established criteria and the expected results to be discussed further.

5. *To strengthen the resilience of regions and local communities it is necessary to form and develop common organizational, security, and other capabilities.* To this end, local authorities are recommended, in particular, to expand the practice of creating citizen safety centers, form a joint network of situational centers at the regional level, to use the potential of regional

development agencies, volunteer organizations, private businesses, and the population for the development of infrastructure of a respective administrative-territorial unit, formation of mutually beneficial partnerships, and the implementation of joint programs.

The building or strengthening of territorial security and defense forces (in particular, territorial defense forces, civil protection forces, and public security forces), implementation of programs to promote support by citizens for law enforcement agencies and civil protection forces on the local level, and the creation of associations of citizens who assist local authorities also contributes to strengthening the resilience of regions and local communities, strengthening existing forces, and developing their organizational capabilities.

A prospective model of coordination and interagency cooperation (at the level of permanent organizational formats) in the field of ensuring the security and resilience of regions and local communities developed based on the above recommendations is presented in *Fig. 5.6.* The idea of implementing such an organizational model is based on theoretical conclusions about the resilience of complex social systems, their ability to effectively resist, recover, and reorganize in response to a crisis as well as their adaptability, which is ensured by the non-linear nature of relationships between the elements of the system. As a result, such a system can quickly adapt to new circumstances and focus on the ability to maintain its basic functions even if the system structure changes or collapses in crisis.



Regional level

Regional, and Kyiv city state administrations

Coordination of activities in the field of regional security and resilience, organization and support functioning of the national systems (and their territorial subsystems) within the relevant administrative unit.

Coordination of activities of district state administrations, territorial subdivisions and offices of state authorities (including NP, SESU, SSSCIP, etc.), SSU, AFU, NGU, enterprises, and organizations at the appropriate administrative ter. unit, etc..

AD

IAWG 1

IAWG 2

IAWG 3

IAWG N

TCC

Executive committees of regional authorities

Providing interaction with LC, local executive authorities, local municipalities

Regional commissions on ensuring security and resilience

Heads of regional and Kyiv city state administrations, representatives of territorial subdivisions of state EA, SSU, AFU, NGU, local authorities, enterprises, institutions and organizations at the appropriate administrative ter. unit

Special regional commissions on emergency response

ATC coordination groups at regional offices of the SSU

Inter-Agency Working Groups on ensuring security and resilience of critical infrastructure

Inter-Agency Working Groups on mobilization and ter. defense

Inter-Agency Working Groups on biosafety and anti-epidemic protection

Inter-Agency Working Groups on other issues of ensuring regional security and resilience

Local educational and methodical courses (specialized and interdepartmental)

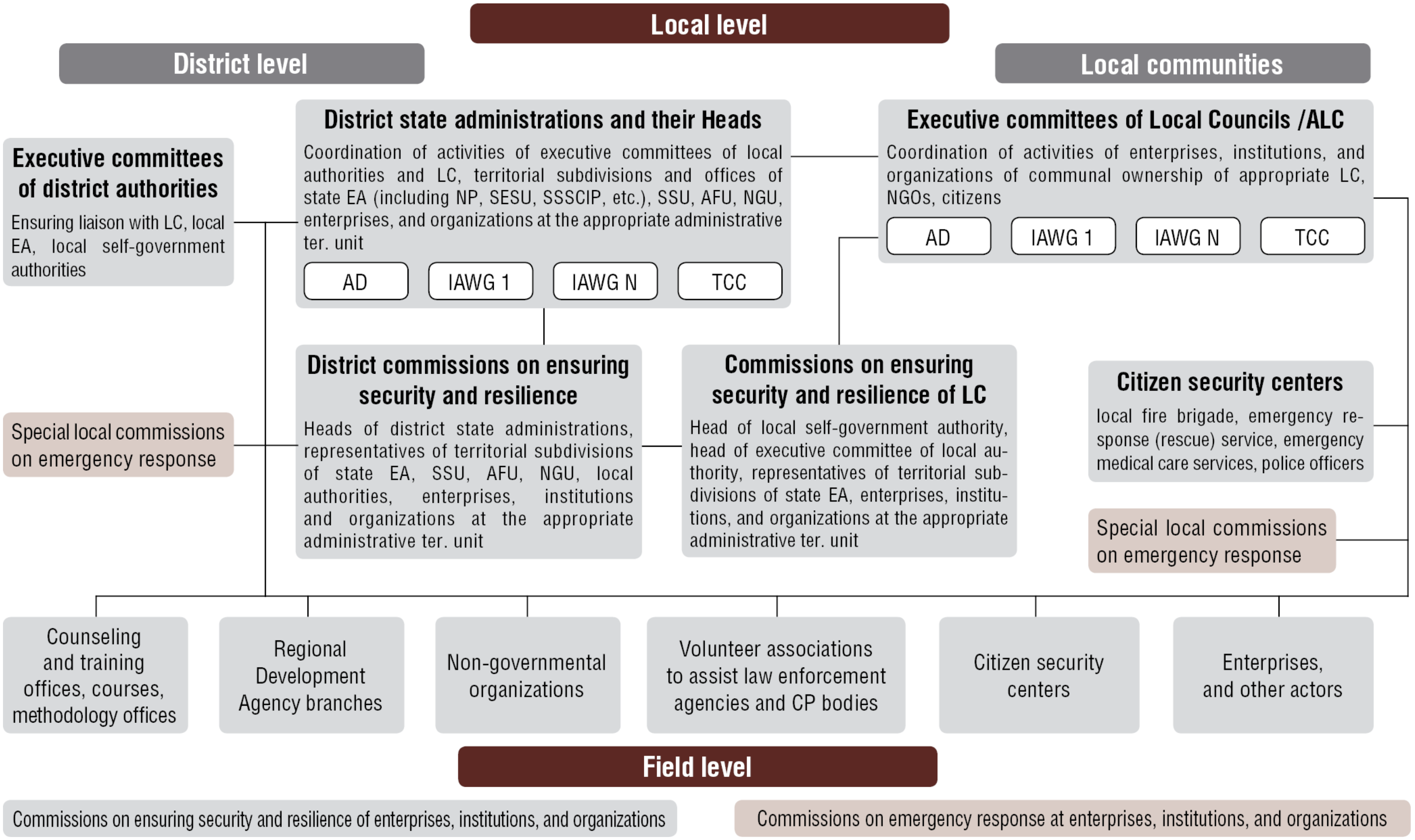
Centers for CP and life safety

Non-governmental organizations

Regional Development Agencies

Volunteer associations to assist law enforcement agencies and CP bodies

Enterprises, and other actors



Executive committees of district authorities

Ensuring liaison with LC, local EA, local self-government authorities

District state administrations and their Heads

Coordination of activities of executive committees of local authorities and LC, territorial subdivisions and offices of state EA (including NP, SESU, SSSCIP, etc.), SSU, AFU, NGU, enterprises, and organizations at the appropriate administrative ter. unit

Executive committees of Local Councils /ALC

Coordination of activities of enterprises, institutions, and organizations of communal ownership of appropriate LC, NGOs, citizens

Special local commissions on emergency response

District commissions on ensuring security and resilience

Heads of district state administrations, representatives of territorial subdivisions of state EA, SSU, AFU, NGU, local authorities, enterprises, institutions and organizations at the appropriate administrative ter. unit

Commissions on ensuring security and resilience of LC

Head of local self-government authority, head of executive committee of local authority, representatives of territorial subdivisions of state EA, enterprises, institutions, and organizations at the appropriate administrative ter. unit

Citizen security centers

local fire brigade, emergency response (rescue) service, emergency medical care services, police officers

Special local commissions on emergency response

Counseling and training offices, courses, methodology offices
Regional Development Agency branches
Non-governmental organizations
Volunteer associations to assist law enforcement agencies and CP bodies
Citizen security centers
Enterprises, and other actors
Field level
Commissions on ensuring security and resilience of enterprises, institutions, and organizations
Commissions on emergency response at enterprises, institutions, and organizations

Notes: *AD – authorized department of the local state administration, IAWG – interagency working groups, TCC – temporary control commission, NP - National Police of Ukraine, SESU - State Emergency Service of Ukraine, SSSCIP - State Service of Special Communications and Information Protection of Ukraine, SSU - Security Service of Ukraine, NGU - National Guard of Ukraine, AFU – Armed Forces of Ukraine, EA - executive authorities, LC - local community, ALC – amalgamated local community , CP - civil protection.*

Fig. 5.6. **Prospective diagram for coordination and interagency interaction in the field of ensuring security and resilience of the regions and territorial communities (on the level of organizational structures of interagency interaction that operate on a permanent basis)**

Source: Reznikova et al., 2021.

The above recommendations on establishing coordination and interagency cooperation in the field of ensuring the security and resilience of regions and local communities envisage amendments to a number of regulatory acts. In particular, due to the need to expand the conceptual and categorical apparatus, clarify functions, tasks, authority, and responsibilities of state executive authorities and local self-government bodies in the field of ensuring national resilience, and introduce new organizational mechanisms for its development, it is necessary to amend the laws of Ukraine “On the National Security of Ukraine,” “On the Cabinet of Ministers of Ukraine,” “On the Foundations of State Regional Policy,” “On Local Governance in Ukraine,” and “On Local State Administrations” as well as many other acts regulating the activities of existing interagency cooperation formats at the territorial level.

Implementation of proposed recommendations will facilitate the following:

- improving planning processes at the territorial level through coordination of strategic priorities, programs, and plans in the areas of socio-economic development, ensuring the security and resilience of regions and local communities;
- updating ministers’ and agencies’ documents on the development of readiness of regions and local communities for certain threats and

emergencies taking into account interagency cooperation on the national, regional, and local levels;

- development and implementation of universal protocols for the enhancement of readiness and response to threats and crises, taking into account their interdependencies and potential cascading effects.

In the context of the above, it is expedient to implement a pilot project on the implementation of the proposed model of organizing activities in the field of ensuring the security and resilience of regions and local communities in one of the regions of Ukraine and several local communities. This requires adoption of a national legal act.

5.5.2. Shaping National Policy in Resilience of Regions and Territorial Communities

The generation of program documents in the field of ensuring the security and resilience of regions and local communities should be consistent with the goals and objectives of the relevant national documents. In addition, these documents should determine specific regional goals and objectives and the expected results and criteria for their evaluation. In accordance with the previously proposed conceptual principles for ensuring national resilience in Ukraine, the main tasks in the field of development of resilience of regions and local communities should be developed following such *goals:*

- thinking paradigm shift – the resilience of regions and local communities is built locally, not in the center;
- generation of an adaptive management model provides for the development of alternative goals and plans for the development of regions and local communities, periodic adjustment of programs and plans depending on the results of risk analysis and trends in the development of the security situation, the definition of targeted guidelines for directed self-management by the communities;
- shaping regional and local leadership;

- introduction of an effective model of coordination and organization of activities in the field of ensuring the resilience of regions and local communities based on whole-of-society cooperation and partnerships;
- ensuring cohesion – uniting citizens around issues of ensuring the security and resilience of regions and local communities;
- generating joint capabilities of regions and local communities to ensure an adequate level of readiness and effective response to threats and a wide range of crises;
- planning improvement – drafting regional and local plans of concerted actions to prevent threats, and ensure readiness, response, and recovery following crises;
- formation of a culture of security by involving citizens and NGOs in programs to support law enforcement agencies and local security centers;
- ensuring effective civil control over the use of resources of regions and communities.

It is appropriate to consider the achievement of the characteristics of a resilient community, which are used, in particular, in the UK. These *main results* should be the focus of relevant state policy,:

- citizens are aware of all the threats and crises that may occur and affect their lives;
- citizens use all acquired skills, knowledge, and existing resources to prepare for the onset of an emergency, its manifestation, and to deal with its consequences;
- citizens adapt their daily skills and knowledge and use them in times of danger;
- communities work in cooperation with local authorities, authorized institutions, and other entities before, during, and after a crisis;
- communities disseminate knowledge among their members about personal protection measures and actions that increase the level of individual

resilience, and share their experiences and positive practices with other communities;

- community members are involved in the decision-making process and are interested in community development and in expanding its capabilities (UK Cabinet Office, 2011).

In addition, dynamics of the development of common capabilities of regions and local communities (organizational, economic, social, and security), effective functioning of interagency cooperation structures in the field of ensuring the security, and resilience of regions and local communities can be determined as important results in the relevant area.

The criteria for achieving the proposed results of developing the resilience of regions and territorial communities should be determined as follows:

Resilience criteria of state:

- reliability and sufficiency of organizational, security, social, and other capabilities of a region or local community;
- availability of reserves of appropriate assets or means;
- cohesion of a community;
- maturity of relations between different social groups;
- involvement of the population in economic, political, and other activities within communities;
- trust in local authorities;

Resilience criteria of functioning:

- the efficiency of regional or community management;
- continuity of public and other critical services to the population, and strategically important business processes within the region or a local community;
- readiness of actors responsible for ensuring the resilience of regions and local communities to respond to threats and crises of different origin and nature;

- controllability of the situation before, during, and after the crisis within a region or a local community;
- quality and accessibility of educational activities in the field of ensuring the security and resilience of a region and a local community;
- awareness by members of a community and the population of a region of nature and the type of threats and the courses of action to be taken in the case they occur;
- involvement of community members in the decision-making process within the relevant administrative-territorial unit;
- reliability and efficiency of bilateral communication channels between local authorities and the population;
- creation of joint capabilities in a region and a local community to counter threats or crises;
- use of new technologies in the field of security environment analysis, risk forecasting, threat detection, and crisis management.

To assess the progress of achieving these criteria, self-assessment questionnaires may be developed based on the recommended list of questions provided in *Annex 3* and based on special indicators. It is recommended to carry out assessments of the capabilities of regions and local communities with consideration of the results of comprehensive and sectoral reviews of the security and defense sector of Ukraine.

Conclusions to Chapter 5

The results of a systems analysis of the security environment of Ukraine, including the mechanisms and practices available in the country in the field of national security and resilience, crisis management, and public administration, indicate the need to create a system for ensuring national resilience in Ukraine. Taking into account the limited national resources, it is expedient to establish such a system by way of strengthening and developing existing systemic ties and implementing the principles of resilience in various spheres of social relations, economic activity, and public administration. Taking into account the identity of the actors and objects of ensuring national security and national resilience on the organizational level, it is worth establishing the national resilience ensuring system, as related to the national security ensuring system of Ukraine. In the future, it is worth considering the possibility of transforming both these systems into a comprehensive one for ensuring national security and resilience.

The introduction of systemic mechanisms for ensuring national resilience in Ukraine primarily requires legislative regulation of the conceptual and institutional foundations of the relevant system functioning. It should be noted that the adoption in Ukraine of the Concept of Support of the National Resilience System is an important step in the development of basic legislation in the relevant area. This regulatory document defined the general idea and organizational model of the national resilience ensuring system in Ukraine, basic characteristics of which correspond to conclusions resulting from the study of the peculiarities of the implementation of the resilience concept in national security, namely:

- such a system should be complex and multi-level, organized at the state, regional, and local levels, which should be based on common principles, key processes, and universal mechanisms for ensuring resilience;
- the system shall respond to a wide range of threats and crises;
- key system processes should cover all stages of the national resilience ensuring cycle;
- systems connections should be arranged based on broad interaction between state and local authorities, representatives of science, business, civil society, and population.

Issues of defining authorities, tasks, and responsibilities of national resilience ensuring actors, in particular state and local authorities, enterprises, and organizations, as well as the procedure for involving representatives of civil society in such activities, improving the interaction between the actors in peacetime, in an emergency, and in wartime require further legal settlement based on the Concept of Support of the National Resilience System in Ukraine.

According to the results of the study, it can be argued that building a national resilience ensuring system in Ukraine should, first of all, include the streamlining of organizational ties between actors rather than the creation of new ministries and agencies. It is expedient to solve the problem of establishing effective coordination and organization of activities in the field of national resilience at different levels by way of clarification of the responsibilities or transforming existing state bodies as well as creating organizational formats for interagency cooperation (interagency working groups, platforms, etc.) without expanding the staff of civil servants.

It is expedient to determine one of the key goals of national policy in the field of national security and resilience in Ukraine as the establishment of a new paradigm of thinking, which states that ensuring national resilience is the responsibility of everyone, not only the state, and that the buildup of the resilience of regions and local communities takes place locally and not in the center. The implementation of this approach will contribute, in particular, to strengthening cohesion in the society, creating the basis for uniting people around issues of ensuring security, resilience, and sustainable development of the state, region, and local community, creating joint capabilities to maintain an adequate level of readiness, and effective response to threats and crises of a wide range. At the same time, this adds relevance to the issue of developing leadership in the state at various levels as well as effective public control over the use of national and local resources for the needs of ensuring national security and resilience.

An urgent task for Ukraine is an introduction of adaptive management, which provides for flexibility and diversity of the national policy in the field of national security and resilience, defining alternative goals and plans at the level of the state, regions, and local communities, implementing directed self-management mechanisms, periodic adjustment of targeted guidelines and plans depending on the results of the analysis and assessment of risks, changes in the security situation, and trends in its development. In this context, it is relevant to create a national system for assessing risks and capabilities and identifying threats and vulnerabilities in Ukraine.

Important for ensuring national resilience in Ukraine is the formation of a culture of security and resilience in the state and in society. This culture would involve the introduction of rules of conduct and skills that would avoid danger or minimize its consequences, and would involve citizens and public organizations in programs to support law enforcement agencies and local security centers.

It can also be stated that planning in Ukraine, as an important element of the national resilience ensuring system, requires improvement of its methodology and organization of relevant processes. The solution of this problem is possible, for example, due to the adoption of the Law of Ukraine "On State Strategic Planning in Ukraine," amendments to the Law of Ukraine "On National Security of Ukraine" in order to determine the full cycle of strategic planning in the field of national security, establishing universal rules to draft strategic planning documents and plan concerted actions in case of large-scale crises with cascading effects; determining the procedures for interagency interaction to include use of various resources (both government and non-government), assets, international assistance at different stages of the national resilience ensuring cycle; clarification of the procedure for monitoring and reporting on the status of implementation of the National Security Strategy of Ukraine and other planning documents in the areas of national security and resilience; and improving the procedure for conducting comprehensive review of the security and defense sector of Ukraine and its components regarding the implementation of the assessment of capabilities and readiness to respond to threats, emergencies, and crises as well as the regular self-assessment of state and local authorities on ensuring resilience to certain threats, emergencies and crises.

CONCLUSIONS

1. Shaping an interdisciplinary concept of resilience and its extension to the field of security research resulted from the development and complementarity of several knowledge fields. At the same time, the growing relevance of national resilience research is indicative of an active search for new methods and ways to respond to modern challenges and threats. The insight into the interdisciplinary concept of resilience, the definition of its characteristics and manifestations as well as the peculiarities of implementation in the field of national security allowed *enhancing and deepening of existing scientific developments, determining the philosophy of resilience in the field of national security, shaping a common theoretical basis for the study of practical mechanisms to ensure national resilience (to include various fields and areas), identifying and characterizing peculiarities of the use of the categorical and conceptual apparatus in the study of various aspects of the development of the system for ensuring national resilience*.

Application of a systems approach to the analysis of the issues of ensuring national resilience made it possible to *propose a definition of "national resilience" which takes into account an integrated approach to countering threats and crises of any nature and origin and also covers the main processes that form the basis of the author's vision of the national resilience ensuring cycle*.

2. The analysis and synthesis of scientific research on the resilience of complex systems, national security, and sustainable development made it possible to determine that the main objects of ensuring national resilience are the state and society as complex systems that have a certain potential for resilience as well as *to scientifically substantiate* that an additional comprehensive organizational mechanism can be formed around these objects. Its functioning is aimed at strengthening the resilience of the state and society to an optimum level under certain conditions, which is a variable value, while avoiding the existing traps.

Besides, *the expediency of building a national resilience ensuring system under changing and uncertain global security environment as well as the need to coordinate the processes of developing and functioning of this system with the national security ensuring system has been proven. It was clarified that a close interaction between these systems allows for synergy. The possibility of combining these systems into a single one for ensuring national security and resilience has been proved.*

3. The study of the nature of the main system elements, connections, and processes in the field of national resilience made it possible to determine and scientifically substantiate the cycle, which is a sequence of actions of the actors in ensuring national resilience. This makes it possible to effectively counter threats of any origin and character, adapt to rapid changes in the security environment, and maintain sustainable functioning of the main spheres of life of a society and the state before, during, and after the crisis. *The practical significance of establishing a national resilience ensuring cycle is that it can be applied while developing a national resilience ensuring system to determine its key processes and the direction of a relevant state policy.*

According to the results of the study of criteria, indicators, levels of ensuring national resilience, and peculiarities of managing relevant processes, *the expediency of implementing adaptive management of national resilience in a changing security environment has been proved.*

The generalized interdisciplinary nature of the author's methodology for assessing national resilience according to the proposed criteria makes it possible to develop special criteria and indicators on its basis to assess resilience in certain areas.

4. The application of a systems approach in the analysis of key elements of the national resilience ensuring system, the links between them, and factors of influence, including from the security environment, combined *allowed to form a generalized multi-level comprehensive model for ensuring national resilience as well as to determine the conceptual foundations for its formation and functioning*

to include basic principles and universal mechanisms. *The practical significance* of this development lies in the fact that based on the proposed universal model and defined regularities, a national resilience ensuring system of each state can be established taking into account its national interests and development features.

It is scientifically substantiated that the highest priority in ensuring national resilience belongs to universal mechanisms and measures aimed at a comprehensive response to a wide range of threats and crises at all stages of the national resilience ensuring cycle.

It is proved that the multi-level system of ensuring national resilience is especially important for countries with a sufficiently large territory and population, to which Ukraine belongs. This is due to the need to establish an effective primary response to threats and crises at the local and regional levels as well as the formation of reliable vertical and horizontal system links.

5. The regularities identified by the results of the study of the theoretical foundations for national resilience helped *determine and characterize the peculiarities of the formation and implementation of a comprehensive state policy in the field of national security and resilience*, in particular, on the application of adaptive management, assessment of risks and capabilities, timely identification of threats and vulnerabilities, strategic analysis and planning, development of plans and protocols of concerted actions in case of crises, the lessons learned of the gained experience, the determination of tasks for ensuring the resilience of society and local communities as well as resilience in certain sectors (spheres), constant monitoring of the security situation to timely amend the established targeted guidelines for the functioning of universal and special mechanisms for ensuring national resilience and clarifications to the relevant state policy.

The obtained results of the study of the methodological tools for ensuring national resilience make it possible to assert the expediency of redistribution of powers in the field of national resilience and security between central and local authorities in which the key role of the state in solving strategic issues of ensuring national security and resilience is preserved as well as the functions of control and coordination that the state performs are strengthened. At the same time, a sufficient amount of powers and resources should be transferred to the regional and local levels. This involves, in particular, the creation or strengthening of territorial security capabilities, the formation of reliable systems links based on broad cooperation, and an increase in social capital.

It has been proved that the implementation of state-defined priorities and tasks in the field of national resilience involves adjusting the daily activities of state and local authorities, developing social solidarity and unity in society, trust in the authorities, establishing reliable bilateral channels of communication between the authorities and the population, and forming an appropriate security culture in the state and society.

6. The results of the analysis and generalization of world experience in ensuring resilience in the field of national and international security suggest that there are no uniform rules in this area. Since ensuring national resilience is the sphere of responsibility of states, they determine the goals, objectives, and priorities of the relevant state policy taking into account national interests, features of historical, cultural, economic, and political development of their country. At the same time, common approaches of different states, their alliances, and international organizations to the implementation of systems elements and mechanisms for ensuring national resilience are based on the essence of the concept of resilience in the field of national security and relevant regularities.

The analysis of strategic and program documents and practices of several states has revealed the changes that have occurred in the national resilience ensuring models: from focusing on priority areas and directions to a broader integrated approach to ensuring readiness to respond to threats of a wide range and effective crisis management based on comprehensive cooperation. It was determined that the biggest changes in the models of ensuring national resilience of various states occurred after 2014.

The results of the analysis of strategic and program documents as well as the recommendations of leading international organizations (the UN, NATO, the

EU, OECD, OSCE) make it possible to conclude a gradual convergence of their conceptual approaches to national resilience. A significant part of the efforts of these organizations is now aimed at eliminating the causes of conflicts, forming a cohesion, trust, and leadership, introducing an integrated approach to ensuring readiness and efficiency of responding to threats of a wide range, rapid recovery of various branches as well as the state and society as a whole after the crisis. *The practical significance* of the conclusions obtained lies in the possibility and expediency of their implementation during the formation and implementation of state policy in the field of ensuring national security and resilience in Ukraine.

Besides, the study of world experiences in ensuring national resilience has made it possible to determine effective world practices in this area that can be applied in Ukraine. In particular, we are talking about the experience of New Zealand in implementing an integrated approach to ensuring national security and resilience; the United Kingdom and the Netherlands – in the formation of national systems for assessing risks and threats as well as the organization of a system for providing the resilience of regions and local communities; the US, Israel, and Japan – in the area of strategic and crisis planning; Scandinavian and the Baltic countries – in the implementation of the whole-of-society approach to the organization of measures in the field of enhancing readiness to respond to threats and recover the state and society after crises.

7. The experience of Ukraine's response to the threats and crises studied suggests that Ukraine's time-tested ability as an independent state to continue functioning in difficult conditions, including under armed aggression by the Russian Federation, the impact of hybrid threats, and crises' of various origins, is evidence of the significant potential for resilience which is embedded both in existing state institutions and mechanisms and in the society. At the same time, current trends in the security environment of Ukraine, the presence of a significant number of threats and vulnerabilities, incomplete compliance of the Ukrainian state and society with the criteria for the resilience of their state and resilience of their functioning *prove the expediency of building a national resilience ensuring*

system in Ukraine, combined with the national security ensuring system as an additional protective mechanism aimed at strengthening the resilience of the state and society.

Extrapolation from defined theoretical regularities of ensuring national resilience contributed to the determination of conceptual principles, main goals, and objectives of creating an appropriate system and shaping a relevant state policy in Ukraine. It is substantiated that the national resilience ensuring system of Ukraine should be complex and multi-level, organized at the state, regional, and local (territorial) levels. All of them should introduce uniform principles, key processes, and universal mechanisms for ensuring resilience, in particular, a national risk assessment system, a multi-level organizational resilience management system, and a system of strategic analysis and planning as an element of adaptive management. *The practical implementation* of the proposed recommendations was the adoption in Ukraine of the Concept of Support of the National Resilience System as a basic legal act in the relevant area. The author of this book participated in the development of the draft concept.

The results of the analysis of the prospects for the implementation of a systems approach to ensuring national security and resilience in Ukraine make it possible to assert that the functioning of the relevant system on a permanent basis can create several *advantages* for the development of the Ukrainian state and society including improving the efficiency of the existing national systems; reducing the volume of human, material and financial losses due to the emergence of threats, the onset of crises of all kinds; consolidation of society, increasing the level of trust in the authorities; strengthening the capacity of resilience of regions and territorial communities, expanding the capacity of local self-governments in the context of preventing and countering threats and crises, and saving the resources of the state and society through their effective use.

It is scientifically substantiated that the introduction of universal and special mechanisms for ensuring national resilience in Ukraine will contribute to the formation of the ability of the state and society to timely identify threats and vulnerabilities, assess risks, prevent or minimize their negative impacts, respond effectively, and quickly and fully recover from crises of all kinds, including but not limited to hybrid threats. In addition, the use of unified methodological approaches and general criteria for assessing resilience will not only allow us to compare the results of resilience assessment in various areas obtained using specific methods but also to conduct a qualitative analysis of the progress and effectiveness of implementation of sectoral measures in the field of national resilience aimed to determine priorities and make adjustments to the relevant state policy, if necessary.

8. The study of the current state of ensuring national resilience in Ukraine made it possible to distinguish a number *of systemic problems* in this area, including: incoherence and inconsistency of certain measures and legal regulation in this area; shortcomings in shaping a relevant state policy and definition of priority tasks for ensuring national resilience in strategic and programmatic documents as part of a single intent; imperfection of planning joint measures to provide readiness to respond to threats and large-scale crises with cascading effects; imperfection of the strategic analysis and planning system; lack of a systems approach to risk management; shortcomings in the methodology and organization of a comprehensive review of the national security and defense sector and its components; ineffectiveness of mechanisms of organization and coordination of actions at the national, regional and local levels in the field of crisis management; and inconsistency of functioning of existing national systems for responding to certain types of threats and risks.

It is substantiated that the settlement of identified problems in the field of national resilience requires the adoption of comprehensive measures based on the Concept of Support of the National Resilience System as a basic regulatory document in the relevant area in Ukraine. It has been determined that the development of national legislation in the area of national resilience presupposes amending several legislative acts of Ukraine (first of all, the Law of Ukraine “On National Security of Ukraine”) on streamlining, strengthening, and developing systemic ties, establishing effective coordination of activities in the field of ensuring national resilience, and improving strategic planning and crisis management.

9. Taking into account the conclusions on the peculiarities of the implementation of the concept of resilience in the field of national security and world experience, recommendations have been developed regarding the shaping and implementation of several universal mechanisms for ensuring national resilience in Ukraine.

In particular, taking into account effective world practices and national peculiarities in the field of state-building, recommendations have been developed for the introduction in Ukraine of a *comprehensive multi-level organizational mechanism for ensuring national resilience*, which is important for the formation of reliable systemic ties based on whole-of-society cooperation. The introduction of such a mechanism does not provide for amendments to the distribution of powers defined by the Constitution of Ukraine between the main branches of state power and to the current administrative-territorial structure of Ukraine but it takes into account the prospects of decentralization and the need to coordinate the functioning of national systems aimed to respond to certain threats and emergencies that exist or emerge.

Based on the practices used in Ukraine and based on the world experience, *recommendations have been developed to create a comprehensive multi-level system for assessing risks and capabilities, identifying threats and vulnerabilities; the ways of its organizational and legal support were identifyed; recommendations for the state and local authorities, and strategically important enterprises and organizations to conduct resilience self-assessment were formulated.*

10. Taking into account theoretical conclusions on the peculiarities of *the formation and implementation of a state policy in the field of national security and resilience, a set of relevant recommendations for Ukraine has been developed*, in particular, on the determination of strategic goals in the field of ensuring national

security and resilience; ways to implement adaptive governance mechanisms; development of public-private partnership in the national security sphere, and security culture in the state and society; improvement of the system of special education in the national security and defense sector, dissemination of knowledge among the population about risks and threats; providing the cohesion of society through the unification of people around issues of ensuring the security, resilience and sustainable development of the state, region, and local community; the formation of leadership at various levels, as well as effective civil control over the use of state and local resources for the needs of national security and resilience.

11. It is expedient to continue interdisciplinary theoretical and applied research in the field of providing resilience in certain areas, considering the specifics of the relevant branches of science as well as the development of indices and indicators for assessing risks, capabilities, and identification of threats. Results of such research should be considered when improving the national resilience ensuring system of Ukraine, which today is at its initial stage of creation but should not be static in the future.

GLOSSARY

Adaptability – the ability of the state and society to withstand destructive influences and adapt to changes in the security environment due to the implementation of certain internal changes that allows the state and society to preserve integrity and continue fulfilling their functions.

Capabilities – a combination of all available resources, forces, and means of the state, society, community, or organization that determines their ability to efficiently respond to threats and crises at all crisis cycle phases, and adapt to the changing security environment.

Crisis – a state characterized by an extreme aggravation of contradictions, significant destabilization of the situation in any field of activity, region, or state, including a significant disruption of the functioning conditions of the main spheres of life of society and the state, that requires the adoption of a set of measures to stabilize the situation and restore the quality of life of the population, the conditions for the functioning of society and the state at a level not lower than the pre-crisis one. The onset of an emergency may be a prerequisite for the development of a crisis.

Global risk – an event that causes a significant negative impact on several countries and branches.

Hybrid threats – a type of threats to national security resulting from a synergistic effect of simultaneous use of conventional and unconventional methods of influence, which are often covert or disguised as other processes within the legal framework.

National resilience – the ability of a state and society to effectively counter threats of any origin and nature, adapt to rapid changes in the security environment, function continuously, including during crises, and quickly recover after crises to the optimal equilibrium under the reasonable conditions.

National resilience ensuring cycle – the sequence of actions of national resilience actors which allows to effectively counter threats of any origin and nature, adapt to changes in the security environment, and maintain continuous functioning of essential life spheres of the society and state before, during, and after a crisis in order to survive and develop.

National resilience ensuring mechanisms – sets of decisions and measures that determine a sequence of certain processes and actions that meet general aims and principles of the national resilience ensuring system`s functioning, and focus on achieving the established level and criteria of resilience by the state, society, and their individual components.

National resilience ensuring system – a comprehensive mechanism of interaction between public and local authorities, institutions, enterprises, NGOs, and people, as well as targeted actions, methods, factors, and mechanisms that safeguard the security and continuous functioning of key spheres of the society and state before, during, and after crises, including through adaptation to threats and rapid changes in the security environment.

National resilience actors (providers) – public and local authorities, enterprises, institutions, organizations, civil society structures, and citizens that initiate or participate in the national resilience providing processes.

National security – protection of national interests and national values from external and internal threats.

National security ensuring system – a combination of interacting national security actors, forces, facilities, methods, factors, and purposeful actions that guarantee preservation and strengthening of national values, protection and progressive development of national interests through timely detection, prevention, localization, neutralization, and overcoming of internal and external threats, as well as through providing the effective functioning of the national security system and its components.

Organizational resilience – the ability of an organization, institution, or enterprise to identify, prepare for, respond to threats, adapt to changes in the security environment, and function steady before, during, and after a crisis for the sake of survival and further development.

Readiness – the ability of a state and society to rapidly and properly respond to threats and crises.

Resilience – an ability of an object (a complex system) to adapt to the action of external stimuli without a significant loss of functionality and destruction of its structure.

Resilience in certain areas – the ability of the state and local authorities to identify threats characteristic to a certain area, prepare and respond to them in cooperation with enterprises, organizations, civil society structures, and population, and maintain continuous functioning of a certain area, development of corresponding capabilities and post-crisis recovery.

Risk – an effect of uncertainty on objectives (ISO, 2018a).

Threat – a potential cause of an unwanted incident, which could result in harm to individuals, assets, a system, or organization, the environment or the community (ISO, 2021).

Vulnerability – the presence of problems, defects, and deficiencies that cause or increase the susceptibility to disruption, systemic damage, and/or susceptibility to negative effects of risks and threats.

REFERENCES

Abel, T., & Stepp, J. R. (2003). A new ecosystems ecology for anthropology. *Conservation Ecology, 7(3),* art. 12. Retrieved from https://www.ecologyandsociety.org/vol7/iss3/art12/

Ackoff, R. (1971). Towards a System of Systems Concepts. *Management Science, 17(11),* 661–671. Retrieved from https://ackoffcenter.blogs.com/ackoff_center_weblog/files/AckoffSystemOfSystems.pdf

Adger, W. N. (2000). Social and ecological resilience: Are they related? *Progress in Human Geography, 24,* 347–364. Retrieved from https://journals.sagepub.com/toc/phgb/24/3

Adger, W. N., Hughes, T. P., Folke, C., Carpenter, S. R., & Rockström, J. (2005). Social-ecological resilience to coastal disasters. *Science, 309*, 1036–1039. Retrieved from https://science.sciencemag.org/content/309/5737/1036

Allwood, J.M., Bosetti, V., Dubash, N.K., Gómez-Echeverri, L., & Stechow, C. von. (2014). Glossary. In O. Edenhofer et al. *Climate Change 2014: Mitigation of Climate Change.* Contribution of Working Group III to the Fifth Assessment Report of the Intergovernmental Panel on Climate Change. Cambridge University Press, Cambridge, United Kingdom and New York, NY, USA. Retrieved from https://www.ipcc.ch/site/assets/uploads/2018/02/ipcc_wg3_ar5_annex-i.pdf

Ashby, W. R. (1947). Principles of the Self-Organizing Dynamic System. *Journal of General Psychology, 37,* 125–128.

Ashby, W. R. (1960). *Design for a brain: the origin of adaptive behavior.* New York: Wiley.

Australian Disaster Resilience Knowledge Hub. (n.d.). *Australian Disaster*

Resilience Glossary. Retrieved from https://knowledge.aidr.org.au/glossary/?wordOfTheDayId=&keywords=&alpha=&page=5&results=50&order=AZ

Balzacq, T. (2005). The three faces of securitization: Political agency, audience, and context. *European Journal of International Relations, 11(2),* 171–201. doi:10.1177/1354066105052960

Barrett, C. B., & Constas, M. A. (2014). Toward a theory of resilience for international development applications. *Proceedings of the National Academy of Sciences of the USA, 111,* 14625–14630. Retrieved from https://www.pnas.org/content/111/40/14625

Belfer Center. (2016). *Deterring Terror. How Israel Confronts the Next Generation of Threats.* Belfer Center Special Report. English Translation of the Official Strategy of the Israel Defense Forces. Belfer Center for Science and International Affairs.

Berkes, F. (2007). Understanding uncertainty and reducing vulnerability: lessons from resilience thinking. *Natural Hazards, 41*, 283–295. Retrieved from https://link.springer.com/article/10.1007/s11069-006-9036-7

Berkes, F., Colding, J., & Folke, C. (2003). *Navigating social-ecological systems: building resilience for complexity and change.* Cambridge: Cambridge University Press. Retrieved from http://assets.cambridge.org/052181/5924/sample/0521815924ws.pdf

Berkes, F., & Ross, H. (2013). Community resilience: toward an integrated approach. *Society & Natural Resources, 26,* 5–20. Retrieved from https://www.tandfonline.com/doi/full/10.1080/08941920.2012.736605?needAccess=true

Bertalanffy, L. von. (1968). *General System Theory: Foundations, Development, Applications.* N.Y.: George Braziller.

Biggs, R., Schlüter, M., & Schoon, M. L. (2015). *Principles for building resilience: sustaining ecosystem services in social-ecological systems.* Cambridge: Cambridge University Press. Retrieved from https://www.cambridge.org/core/books/principles-for-building-resilience/578EBCAA6C9A18430498982D66CFB042

Bogdanov, A.A. (2003). *Tektolohiia: Vseobschaya organizatsionnaya nayka* [Tectology: universal organizational science]. Moscow: FINANSY. [in Russian]

Bohdanovych, V.Yu., Semenchenko, A.I., & Yezheyev, M.F. (2008). *Metody derzhavnoho upravlinnia zabezpechenniam natsionalnoi bezpeky u ii vyznachalnykh sferakh* [Methods for public administration of ensuring national security in its key spheres]. Kyiv: NADU. [in Ukrainian]

Bohle, H. G., Etzold, B., & Keck, M. (2009). *Resilience as agency*. Retrieved from https://www.researchgate.net/profile/Markus-Keck/publication/263111355_Resilience_as_Agency/links/0a85e539eed4c4a472000000/Resilience-as-Agency.pdf

Booth, K. (1991). Security and Emancipation. *Review of International Studies, 17(4).* 313–326.

Borisoglebsky, D., Naghshbandi, S. N., & Varga, L. (2019). *Analytical approaches to resilience*. Retrieved from https://nic.org.uk/app/uploads/Analytical-approaches-to-resilience-07.08.2019-clean_Final.pdf

Boucher, J. A. (2009). *National Security Policies and Strategies: A Note on Current Practice*. Stimson Center. Retrieved from https://www.stimson.org/wp-content/files/file-attachments/Stimson_National_Security_Strategy_Note_FINAL_12dec09_1_1.pdf

Bourbeau, P. (2013). Resiliencism: premises and promises in securitization research. *Resilience, 1(1),* 3–17.

Bowles, S., Durlauf, S., & Hoff, K. (Eds.) (2006). *Poverty traps.* Princeton: Princeton University Press.

Boyko, A.V. (2014). *Stiykist natsionalnoi ekonomiky: teoriia, metodolohiia, praktyka* [National economics resilience: theory, methodology, practice].

Kyiv: National Academy of Science of Ukraine. [in Ukrainian]

Brand, F. S., & Jax, K. (2007). Focusing the meaning(s) of resilience: resilience as a descriptive concept and a boundary object. *Ecology and Society, 12(1),* art. 23. Retrieved from http://www.ecologyandsociety.org/vol12/iss1/art23/

Brauch, H. G. (2005). Threats, Challenges, Vulnerabilities and Risks in Environmental and Human Security. *Studies of the University: Research, Counsel, Education, 1*. Bonn: United Nation University, Institute for Environment and Human Security.

Brauch, H. G. (2011). Concepts of Security Threats, Challenges, Vulnerabilities, and Risks. In H. G. Brauch, et al. (Eds.), *Coping with Global Environmental Change, Disasters and Security*. (pp. 61–106). Hexagon Series on Human and Environmental Security and Peace.

Breedlove, F. M. (2015). Foreword. In G. Lasconjarias & J. A. Larsen (Eds.), *NATO's Response to Hybrid Threats*. NATO Defense College.

Brown, D., & Kulig, J. (1996/97). The concept of resilience: Theoretical lessons from community research. *Health and Canadian Society, 4,* 29–52.

Brown, H. (1983). *Thinking about National Security: Defense and Foreign Policy in a Dangerous World.* Boulder: Westview Press.

Brown, K. (2014). Global environmental change I: a social turn for resilience? *Progress in Human Geography, 38,* 107–117. doi:10.1177/0309132513498837

Buzan, B., & Waever, O. (1998). *Security: A New Framework for Analysis.* Boulder: Lynne.

Cabinet of Ministers of Ukraine. (2014). *Pro zatverdzhennia Polozhennia pro yedynu derzhavnu systemu tsyvilnoho zakhystu* [On approving the Regulation on unified national civil defense system]. Resolution of the Cabinet of Ministers of Ukraine No 11. Retrieved from https://zakon.rada.gov.ua/laws/show/11-2014-п#Text [in Ukrainian].

Cabinet of Ministers of Ukraine. (2015). *Pro Derzhavnu komisiiu z pytan tekhnohenno-ekolohichnoi bezpeky ta nadzvychainykh sytuatsii* [On the

State Committee on technogenic and environmental security and emergencies]. Resolution of the Cabinet of Ministers of Ukraine No 18. Retrieved from https://zakon.rada.gov.ua/laws/show/18-2015-%D0%BF#Text [in Ukrainian].

Cabinet of Ministers of Ukraine. (2016). *Pro zatverdzhennia Polozhennia pro yedynu derzhavnu systemu zapobihannia, reahuvannia i prypynennia terorystychnykh aktiv ta minimizatsii yikh naslidkiv* [On approving the Regulation on unified national system for preventing, responding to and neutralizing terrorist acts and mitigating their consequences]. Resolution of the Cabinet of Ministers of Ukraine No 92. Retrieved from https://zakon.rada.gov.ua/laws/show/92-2016-п#Text [in Ukrainian].

Cabinet of Ministers of Ukraine. (2017a). *Pro skhvalennia Kontseptsii stvorennia derzhavnoi systemy zakhystu krytychnoi infrastruktury* [On Approving the Concept for Establishing a National Critical Infrastructure Protection System]. Order of the Cabinet of Ministers of Ukraine No 1009-р. Retrieved from https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#Text [in Ukrainian].

Cabinet of Ministers of Ukraine. (2017b). *Pro zatverdzhennia Poriadku rozroblennia planiv diialnosti yedynoi derzhavnoi systemy tsyvilnoho zakhystu* [On approving the Procedures for developing action plans for the unified national civil defense system]. Resolution of the Cabinet of Ministers of Ukraine No 626. Retrieved from https://zakon.rada.gov.ua/laws/show/626-2017-п#Text [in Ukrainian].

Cabinet of Ministers of Ukraine. (2018). *Pro zatverdzhennia Poriadku provedennia oboronnoho ohliadu Ministerstvom oborony* [On approving the Procedures of conducting defense review by the Ministry of Defense]. Resolution of the Cabinet of Ministers of Ukraine No 941. Retrieved from https://zakon.rada.gov.ua/laws/show/941-2018-%D0%BF#Text [in Ukrainian].

Cabinet of Ministers of Ukraine. (2019a). *Pro skhvalennia Kontseptsii rozvytku* *systemy ekstrenoi medychnoi dopomohy* [On Approving the Concept of Developing Emergency Medical Care System]. Order of the Cabinet of Ministers of Ukraine No 383-p. Retrieved from https://zakon.rada.gov.ua/laws/show/383-2019-%D1%80#n8 [in Ukrainian].

Cabinet of Ministers of Ukraine. (2019b). *Pro skhvalennia Stratehii intehrovanoho upravlinnia kordonamy na period do 2025 roku* [On Approving the Strategy for Integrated Border Management until 2025]. Order of the Cabinet of Ministers of Ukraine No 687-p. Retrieved from https://zakon.rada.gov.ua/laws/show/687-2019-%D1%80#n13 [in Ukrainian].

Cabinet of Ministers of Ukraine. (2019c). *Pro zatverdzhennia Poriadku provedennia ohliadu oboronno-promyslovoho kompleksu* [On approving the Procedures of conducting review of the defense and industrial complex]. Resolution of the Cabinet of Ministers of Ukraine No 490. Retrieved from https://zakon.rada.gov.ua/laws/show/490-2019-%D0%BF#Text [in Ukrainian].

Cabinet of Ministers of Ukraine. (2020a). *Pro zatverdzhennia Derzhavnoi stratehii rehionalnoho rozvytku na 2021-2027 roky* [On approving the State Regional Development Strategy during 2021-2027]. Resolution of the Cabinet of Ministers of Ukraine No 695. Retrieved from https://zakon.rada.gov.ua/laws/show/695-2020-%D0%BF#Text [in Ukrainian].

Cabinet of Ministers of Ukraine. (2020b). *Pro zatverdzhennia planu zakhodiv shchodo realizatsii Kontseptsii rozvytku systemy ekstrenoi medychnoi dopomohy* [On approving action plan to implement the Emergency medical care system development concept]. Order of the Cabinet of Ministers of Ukraine No 111-p. Retrieved from https://zakon.rada.gov.ua/laws/show/111-2020-%D1%80#n33 [in Ukrainian].

Cabinet of Ministers of Ukraine. (2020c). *Pro zatverdzhennia Poriadku* *provedennia ohliadu stanu kiberzakhystu krytychnoi informatsiinoi infrastruktury, derzhavnykh informatsiinykh resursiv ta informatsii, vymoha shchodo zakhystu yakoi vstanovlena zakonom* [On approving the Procedures of conducting review of the cybersecurity status for critical information infrastructure, government information resources and information that is required to be protected by the legislation]. Resolution of the Cabinet of Ministers of Ukraine No 1176. Retrieved from https://zakon.rada.gov.ua/laws/show/1176-2020-%D0%BF#Text [in Ukrainian].

Canetti, D., Waismel-Manor, I., Cohen, N., & Rapaport, C. (2013). What Does National Resilience Mean in a Democracy? Evidence from the United States and Israel. *Armed Forces & Society, 40(3),* 504–520.

Carpenter, S. R., & Brock, W. A. (2008). Adaptive capacity and traps. *Ecology and Society, 13(2),* art. 40. Retrieved from http://www.ecologyandsociety.org/vol13/iss2/art40/

Carpenter, S. R., Brock, W. A., Folke, C., Nes, E. H. van, & Scheffer, M. (2015). Allowing variance may enlarge the safe operating space for exploited ecosystems. *Proceedings of the National Academy of Sciences of the USA, 112,* 14384–14389. Retrieved from https://www.pnas.org/content/112/46/14384

Carpenter, S. R., Folke, C., Olsson, O., Schultz, L., Balvanera, P., Campbell, B. M., … Spierenburg, M. (2012). Program on ecosystem change and society: an international research strategy for integrated social-ecological systems. *Current Opinion in Environmental Sustainability, 4,* 134–138. Retrieved from https://www.researchgate.net/publication/224852295_Program_on_ecosystem_change_and_society_An_international_research_strategy_for_integrated_social-ecological_systems

Carpenter, S., Walker, B., Anderies, J. M., & Abel, N. (2001). From metaphor to measurement: resilience of what to what? *Ecosystems, 4(8),* 765– 781.

Caudle, S. L., & Spiegeleire, S. de. (2010). A New Generation of National Security Strategies: Early Findings from the Netherlands and the United Kingdom. *Journal of Homeland Security and Emergency Management, 7(1),* art. 35. Retrieved from https://doi.org/10.2202/1547-7355.1679

Center for the Protection of National Infrastructure. (2021). *Security Culture.* Retrieved from https://www.cpni.gov.uk/security-culture

Chandler, D. (2012). Resilience and human security: The post-interventionist paradigm. *Security Dialogue, 43(3),* 213–229.

Chandler, D. (2014). Beyond neoliberalism: resilience, the new art of governing complexity. *Resilience, 2(1),* 47–63.

Cherniatevych, Ya. V. (2012). Situational Center. In H.P. Sytnyk (Ed), *Hosudarstvennoe upravlenie v sfere natsionalnoi bezopasnosti: slovar-spravochnyk* [Public administration in the national security area: glossary-reference book] (pp. 362–365). Kyiv: NADU. [in Ukrainian].

Churchman, C. W., & Ratoosh, P. (Eds.). (1959). *Measurement: Definitions and Theories.* New York: John Wiley.

City resilience index. (n.d.). Arup. Retrieved from https://www.cityresilienceindex.org/

Community and Regional Resilience Institute [CARRI] (2013). *Definitions of Community Resilience: An Analysis.* A CARRI Report. Retrieved from https://s31207.pcdn.co/wp-content/uploads/2019/08/Definitions-of-community-resilience.pdf

Corning, P. A. (2002). The Re-Emergence of "Emergence": A Venerable Concept in Search of a Theory. *Complexity, 7(6),* 18–30. Retrieved from https://onlinelibrary.wiley.com/doi/epdf/10.1002/cplx.10043

Council of Australian Governments. (2015). *Strengthening Our Resilience.* Australia’s Counter-Terrorism Strategy. Retrieved from https://www.nationalsecurity.gov.au/Media-and-publications/Publications/Documents/Australias-Counter-Terrorism-Strategy-2015.pdf

Council of the European Union. (2003). *A Secure Europe in a Better World.* European Security Strategy. Retrieved from https://data.consilium.europa.eu/doc/document/ST-15895-2003-INIT/en/pdf

Council of the European Union. (2013). *Council Conclusions on EU Approach to Resilience.* Brussels. Retrieved from https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/foraff/137319.pdf

Council of the European Union. (2016). *Implementation Plan on Security and Defence.* Retrieved from https://data.consilium.europa.eu/doc/document/ST-14392-2016-INIT/en/pdf

Council of the European Union. (2020). *Proposal for a Regulation of the European Parliament and of the Council establishing a Recovery and Resilience Facility.* No 2020/0104 (COD). Brussels. Retrieved from https://data.consilium.europa.eu/doc/document/ST-14310-2020-INIT/en/pdf

Crane, T. A. (2010). Of models and meanings: cultural resilience in social-ecological systems. *Ecology and Society, 15(4),* art. 19. Retrieved from https://ecologyandsociety.org/vol15/iss4/art19/

Curtin, C. G., & Parker J. P. (2014). Foundations of resilience thinking. *Conservation Biology, 28,* 912–923. Retrieved from https://conbio.onlinelibrary.wiley.com/doi/abs/10.1111/cobi.12321

Dillon, M. & Neal, A. (Eds.). (2008). *Foucault on Politics, Security and War.* Palgrave Macmillan. Retrieved from https://www.researchgate.net/profile/Andrew-Neal/publication/267206491_Foucault_on_Politics_Security_and_War/links/54e39d060cf2b2314f5de23b/Foucault-on-Politics-Security-and-War.pdf

Disaster Recovery Institute. (n.d.). *International Glossary for Resilience*. Retrieved from https://drii.org/resources/viewglossary

Domaryev, V.V. (2017). *Systema sytuatsiynoho upravlinnia: teoriia, metodolohiya, rekomendatsii* [Situational control system: theory, methodology, recommendations]. Kyiv: Znannia Ukrainy. [in Ukrainian]

Donno, R. (2017). *Building national resilience: Survive crisis, seize opportunity, prepare for change*. Booz Allen Hamilton, Inc. Retrieved from https://www.boozallen.com/content/dam/boozallen_site/dig/pdf/white_paper/building-national-resilience.pdf

Duit, A., Galaz, V., Eckerberg, K., & Ebbesson, J. (2010). Governance, complexity, and resilience. *Global Environmental Change, 20,* 363–368. Retrieved from https://www.sciencedirect.com/science/article/abs/pii/S095937801000035X?via%3Dihub

Edwards, C. (2009). *Resilient Nation*. London: Demos.

Eisenkot, G., & Siboni, G. (2019). *Guidelines for Israel's National Security Strategy*. The Washington Institute for Near East Policy.

Erikson, K. T. (1995). *A new species of trouble: the human experience of modern disasters*. New York: W. W. Norton.

European Commission. (2012). *The EU approach to resilience: learning from food security crises*. Communication from the Commission to the European Parliament and the Council. Brussels. Retrieved from https://ec.europa.eu/echo/files/policies/resilience/com_2012_586_resilience_en.pdf

European Commission. (2014a). *Building resilience: the EU's approach*. Retrieved from https://reliefweb.int/sites/reliefweb.int/files/resources/EU_building_resilience_en.pdf

European Commission. (2014b). *The EU Approach to Resilience: Learning from Food Security Crises*. Factsheet. Retrieved from https://ec.europa.eu/echo/files/aid/countries/factsheets/thematic/resilience_africa_en.pdf

European Commission. (2016a). *Action Plan on the Sendai Framework for Disaster Risk Reduction 2015–2030. A disaster risk-informed approach for all EU policies*. Commission staff working document No

SWD(2016)205final/2. Brussels. Retrieved from https://ec.europa.eu/echo/sites/default/files/1_en_document_travail_service_part1_v2.pdf

European Commission. (2016b). *Building resilience: the EU's approach*. Factsheet. Retrieved from https://ec.europa.eu/echo/files/aid/countries/factsheets/thematic/EU_building_resilience_en.pdf

European Commission. (2016c). *Joint Framework on countering hybrid threats: a European Union response.* Joint Communication to the European Parliament and the Council No JOIN(2016)18final. Brussels. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018

European Commission. (2018). *Tackling online disinformation: a European Approach.* Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions No COM(2018)236final. Brussels. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236

European Commission. (2021). *Guidance to member states recovery and resilience plans.* Commission staff working document No SWD(2021)12final. Brussels. Retrieved from https://ec.europa.eu/info/sites/default/files/document_travail_service_part1_v2_en.pdf

European Council. (1996). Council Regulation concerning humanitarian aid (EC) No 1257/96 of 20 June 1996. *Official Journal of the European Union*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31996R1257&from=EN

European Council. (2016). Council Regulation on the provision of emergency support within the Union No 2016/369 of 15 March 2016. *Official Journal of the European Union*. Retrieved from https://eur- https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0369&from=EN

European Council. (2020a). *Joint statement of the Members of the European Council*. Brussels. Retrieved from https://www.consilium.europa.eu/media/43076/26-vc-euco-statement-en.pdf

European Council. (2020b). *Roadmap for recovery. Towards a more resilient, sustainable and fair Europe*. Retrieved from https://www.consilium.europa.eu/media/43384/roadmap-for-recovery-final-21-04-2020.pdf

European Parliament and Council. (2013). Decision No 1313/2013/EU of the European Parliament and of the Council on a Union Civil Protection Mechanism, 17 December 2013. *Official Journal of the European Union*. Retrieved from https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:347:0924:0947:EN:PDF

European Parliament and the Council. (2016). *Joint Framework on countering hybrid threats: a European Union response.* Joint Communication to the European Parliament and the Council. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018

European Parliament and the Council. (2017). *A Strategic Approach to Resilience in the EU's external action.* Joint Communication to the European Parliament and the Council. Brussels. Retrieved from https://eeas.europa.eu/sites/default/files/join_2017_21_f1_communication_from_commission_to_inst_en_v7_p1_916039.pdf

European Parliament and Council. (2021a). Regulation (EU) 2021/241 of the European Parliament and of the Council of 12 February 2021 establishing the Recovery and Resilience Facility. *Official Journal of the European Union*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R0241&from=EN

European Parliament and Council. (2021b). Regulation (EU) 2021/888 establishing the European Solidarity Corps Programme and repealing

Regulations (EU) 2018/1475 and (EU) No 375/2014. *Official Journal of the European Union*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R0888&from=en

European Parliament. (2017). *Resilience as a Strategic Priority of the External Action of the EU*. Resolution 2017/2594(RSP). Brussels. Retrieved from https://www.europarl.europa.eu/doceo/document/TA-8-2017-0242_EN.html

European Union. (2007). Treaty of Lisbon. Amending the Treaty on European Union and the Treaty establishing the European Community. Signed at Lisbon, 13 December 2007. *Official Journal of the European Union*. Retrieved from http://publications.europa.eu/resource/cellar/688a7a98-3110-4ffe-a6b3-8972d8445325.0007.01/DOC_19

European Union. (2016). *A Global Strategy for the European Union's Foreign and Security Policy. Shared Vision, Common Action: A Stronger Europe.* Retrieved from https://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf

Evans B., & Reid J. (2015). Exhausted by resilience: response to the commentaries. *Resilience, 3(2),* 154–159.

Faruqee H., & Pescatori A. (2013). *How to build resilience in Canada's financial sector.* World Economic Forum. Retrieved from https://www.weforum.org/agenda/2015/03/how-to-build-resilience-in-canadas-financial-sector

Federal Emergency Management Agency [FEMA]. (n.d.a). *FEMA Glossary.* Retrieved from https://www.fema.gov/about/glossary

Federal Emergency Management Agency [FEMA]. (n.d.b). *FEMA Resilience.* Retrieved from https://www.fema.gov/about/offices/resilience

Fiksel, J. (2003). Designing Resilient, Sustainable Systems. *Environmental Science and Technology, 37 (23),* 5330–5339. Retrieved from http://www.ask-force.org/web/Sustainability/Fiksel-Designing-Resilient-Sustainable-Systems-2003.pdf

Fiksel, J. (2006). Sustainability and resilience: toward a systems approach.

Sustainability: Science, Practice and Policy, 2(2), 14–21.

Fjäder, C. (2014). The nation-state, national security and resilience in the age of globalization. *Resilience, 2(2),* 114–129.

Fluri, F. & Badrak, V. (2017). *Bezpekovi aspekty politychnoi detsentralizatsii v Ukraini: bachennia, realii ta mozhlyvosti* [Security aspects of political decentralization in Ukraine: vision, realia and capabilities]. Geneva, Kyiv: Center for army, conversion and disarmament research. [in Ukrainian].

FM Global. (n.d.). FM Global resilience index. Retrieved from http://www.fmglobal.com/resilienceindex

Folke, C. (2016). Resilience (Republished). *Ecology and Society, 21(4),* art. 44. Retrieved from http://www.ecologyandsociety.org/vol21/iss4/art44/

Folke, C., & Boyd, E. (Eds.). (2011). *Adapting institutions: governance, complexity and social-ecological resilience.* Cambridge: Cambridge University Press. Retrieved from https://www.cambridge.org/core/books/adapting-institutions/786FFF7911899FE87642F193575EA31F

Food and Agriculture Organization [FAO]. (n.d.). *Resilience Programme in Somalia*. Retrieved from http://www.fao.org/emergencies/fao-in-action/projects/detail/en/c/265285/

Francart, L. (2010). *What does resilience really mean?* Retrieved from https://www.diploweb.com/What-does-resilience-really-mean.html

GLOBSEC Bratislava forum. (2021). *Strategic foresight for resilience: the EU and NATO in a post-pandemic world.* Session summary. Retrieved from https://www.forum.globsec.org/key-message/12305/session-summary-strategic-foresight-for-resilience-the-eu-and-nato-in-a-post-pandemic-world

Government of Canada. (2013). *Building Resilience against Terrorism.* Canada's Counter-Terrorism Strategy. Retrieved from https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rslnc-gnst-trrrsm/index-en.aspx

Guilbert, K. (2015, November 16). *Why West Africa needs to build resilience.*

World Economic Forum. Retrieved from https://www.weforum.org/agenda/2015/11/why-west-africa-needs-to-build-resilience

Gunderson, L. H., & Holling, C. S. (Eds). (2001). *Panarchy: Understanding Transformations in Systems of Humans and Nature*. Island Press.

Gunderson, L. H., Holling, C. S.,& Light S. S. (1995). *Barriers and Bridges to the Renewal of Ecosystems and Institutions*. New York: Columbia University Press.

Habron, G. (2003). Role of Adaptive Management for Watershed Councils. *Environmental Management, 31(1),* 29–41.

Hamilton, A. (1788). Concerning the Militia. *The Federalist, 29*. Retrieved from https://www.constitution.org/fed/federa29.htm

Hartmann, U. (2017). The Evolution of the Hybrid Threat, and Resilience as a Countermeasure. *Research Paper of the Research Division – NATO Defense College, 139.* Retrieved from https://www.ndc.nato.int/news/news.php?icode=1083

Hayek, F. A. (1967). The Theory of Complex Phenomena. In F. A. Hayek*, Studies in Philosophy, Politics and Economics* (pp. 22–42). London: Routledge & Kegan Paul.

Hayek, F. A. (1991). The Fatal Conceit: The Errors of Socialism. In *The collected Works of F. A. Hayek. Vol. 1*. University of Chicago Press.

Held, D., & McGrew, A. (1998). The End of the Old Order? Globalization and the Prospects for World Order. *Review of International Studie, 24(4),* 219– 245.

Hlushak, O.M. (2019). Dosvid vprovadzhennia ryzykooriyentovanoho planuvannia ta kultury bezpeky v orhanah i pidrozdilakh natsionalnoi politsii Ukrainy [Experience of introducing risk based planning and security culture in the Ukrainian National Police units and organizations]. In *Development of civil defense in modern security environment* (pp. 68–75). Proceedings of the International Conference, Kyiv, October 8, 2019. [in Ukrainian].

Hodicky, J., Özkan, G., Özdemir, H., Stodola, P., Drozd, J., & Buck W. (2020). *Dynamic Modeling for Resilience Measurement: NATO Resilience Decision Support Model.* Retrieved from http://dx.doi.org/10.3390/app10082639

Holling, C. S. (1973). Resilience and Stability of Ecological Systems. *Annual Review of Ecology and Systematics, 4,* 1–23.

Holling, C. S. (1978). *Adaptive Environmental Assessment and Management.* London: Wiley.

Holling, C. S. (2001). Understanding the Complexity of Economic, Ecological, and Social Systems. *Ecosystem, 4,* 390–405.

Holmes, K. R. (2014). *What is National Security?* The Heritage Foundation. Retrieved from https://www.heritage.org/military-strength-topical-essays/2015-essays/what-national-security

Horbulin, V.P. (Ed.). (2017). *Svitova hibrydna viyna* [Global hybrid war]. Kyiv: NISS. [in Ukrainian].

Horbulin, V.P., & Kachynskyi, A.B. (2009). *Zasady natsionalnoi bezpeky Ukrainy* [Foundations of the National Security of Ukraine]. Kyiv: Intertekhnolohiya. [in Ukrainian].

Horbulin, V.P., & Kachynskyi, A.B. (2010). *Stratehichne planuvannia: vyrishennia problem natsionalnoi bezpeky* [Strategic planning: solution to national security issues]. Kyiv: National Institute for Strategic Studies. [in Ukrainian].

Horbulin, V.P., Vlasiuk, O.S., Libanova, E.M., & Liashenko, O.M. (Eds.). (2015). *Donbas i Krym tsina povernennia* [Donbas and Crimea: cost of return]. Kyiv: National Institute of Strategic Studies. [in Ukrainian].

IBM. (2009). *Business continuity and resilience services from IBM.* N.Y.: Somers. Retrieved from https://www.ciosummits.com/media/pdf/cloud/IBM_strengthen_your_business.pdf

Ilko Kucheriv democratic initiatives foundation [DIF]. (2018). *Hromadianske suspilstvo u 2018: novi vyklyky, novi zavdannia* [Civil society in 2018: new challenges, new tasks]. A public discussion devoted to the 25th anniversary of the Democratic Initiatives fund by name of Ilko Kucheriv. Retrieved from https://dif.org.ua/uploads/pdf/13963398165a9eef1b022177.77359526.pdf [in Ukrainian].

ISO. (2007a). *Societal security – Guideline for incident preparedness and operational continuity management.* ISO/PAS 22399:2007. Retrieved from https://www.iso.org/standard/50295.html

ISO. (2007b). *Specification for security management systems for the supply chain.* ISO 28000:2007. Retrieved from https://www.iso.org/standard/44641.html

ISO. (2013) *Information technology – Security techniques – Information security management systems – Requirements.* ISO/IEC 27001:2013. Retrieved from https://www.iso.org/standard/54534.html

ISO. (2016). *Sustainable development in communities – Management system for sustainable development – Requirements with guidance for use*. ISO 37101:2016. Retrieved from https://www.iso.org/standard/61885.html

ISO. (2017a). *Organizational resilience – Principles and attributes.* ISO 22316:2017. Security and resilience. Retrieved from https://www.iso.org/standard/50053.html

ISO. (2017b). *Security and resilience – Organizational resilience – Principles and attributes.* ISO 22316:2017. Retrieved from https://www.iso.org/obp/ui#iso:std:iso:22316:ed-1:v1:en

ISO. (2018a). *Risk management – Guidelines.* ISO 31000:2018. Retrieved from https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en

ISO. (2018b). *Security and resilience – Community resilience – Guidelines for supporting vulnerable persons in an emergency*. ISO 22395:2018. Retrieved from https://www.iso.org/standard/50291.html

ISO. (2018c). *Sustainable cities and communities – Indicators for city services and quality of life*. ISO 37120:2018. Retrieved from https://www.iso.org/standard/68498.html

ISO. (2019a). *Risk management – Risk assessment techniques*. IEC 31010:2019. Retrieved from https://www.iso.org/standard/72140.html

ISO. (2019b). *Security and resilience – Business continuity management systems – Requirements*. ISO 22301:2019. Retrieved from https://www.iso.org/standard/75106.html

ISO. (2019c). *Sustainable cities and communities – Indicators for resilient cities.* ISO 37123:2019. Retrieved from https://www.iso.org/standard/70428.html

ISO. (2019d). *Sustainable cities and communities – Indicators for smart cities.* ISO 37122:2019. Retrieved from https://www.iso.org/standard/69050.html

ISO. (2020). *Security and resilience – Community resilience – Guidelines for conducting peer reviews.* ISO 22392:2020. Retrieved from https://www.iso.org/standard/50289.html

ISO. (2021). *Security and resilience – Vocabulary.* ISO 22300:2021. Retrieved from https://www.iso.org/obp/ui/#iso:std:iso:22300:ed-3:v1:en:term:3.1.162

James, P. (1996). *Nation Formation. Towards a Theory of Abstract Community.* SAGE Publications. London. Vol. I. Retrieved from https://www.academia.edu/40353321/Nation_Formation_Towards_a_Theory_of_Abstract_Community_Vol._I_1996

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, July 08). Retrieved from https://www.nato.int/cps/en/natohq/official_texts_133163.htm

Jones, R. W. (1999). *Security, Strategy and Critical Theory*. London : Lynne Rienner Publishers.

Joseph, J. (2013). Resilience as embedded neoliberalism: a governmentality approach. *Resilience, 1(1),* 38–52.

Jovanovich, A. S., Klimek, P., Linkov, I., Sanne, J. M., Székely, Z., Vollmer, M., …Walther, G. (2016). *Analysis of existing assessment resilience approach, indicators and data sources: Usability and limitations of existing indicators* *for assessing, predicting and monitoring critical infrastructure resilience.* Stuttgart. Retrieved from https://www.researchgate.net/publication/316548433

Kachynskyi, A.B. (2015). Indykator mohutnosti yak intehralnyi pokaznyk bezpeky derzhavy [Power indicator as an integrated index of national security]. *Matematychne modeluvannia v ekonomitsi* [Mathematical modeling in economics], *2,* 75–91. [in Ukrainian].

Kaplan, Yu.B. (2016). *Kliuchovi zasady derzhavnoi polityky u sferi zabezpechennia prav i svobod bnutrishnio peremischenykh osib* [Key foundations of the national policy with regard to supporting rights and freedoms of the internally displaced people]. Kyiv: NISS. Retrieved from https://niss.gov.ua/doslidzhennya/politika/klyuchovi-zasadi-derzhavnoi-politiki-u-sferi-zabezpechennya-prav-i-svobod [in Ukrainian].

Kaufmann, M. (2013). Emergent self-organisation in emergencies: resilience rationales in interconnected societies. *Resilience, 1(1),* 53–68.

Kaufmann M., Cavelty, M. D., & Kristensen, K. S. (2015). Resilience and (in)security: Practices, subjects, temporalities. *Security Dialogue, 46(1),* 3–14.

Kharazishvili, Yu.M. (2019). *Systemna bezpeka staloho rozvytku: instrumentariy otsinky, reservy ta stratehichni stsenarii realizatsii* [Systematic security of a sustained development: assessment tools, reserves and strategic implementation scenarios]. Kyiv: National Academy of Science of Ukraine. [in Ukrainian].

Korniyevskyi, O. (2011). National security. In Yu. Levenets, Yu. Shapoval (Eds.) *Politychna entsyklopedia* [Political encyclopedia] (pp. 489–490). Kyiv: Parlamentsky vydavnytstvo. [in Ukrainian].

Kovalivska, S.V. (2020). Koordinatsiia diy mistsevykh orhaniv vykonavchoi vlady ta orhaniv mistsevoho samovriaduvannia u sferi zdiysnennia protyepidemichnykh zakhodiv [Coordination of local executive authorities and local governments in the area of implementing epidemic control measures]. Kyiv: NISS. Retrieved from https://niss.gov.ua/sites/default/files/2020-08/mistsevi-organy-covid_0.pdf [in Ukrainian].

Kovalivska, S.V., Barynova, S.V., & Nesterenko, V.V. (2020). Schodo ryzykiv dlia nalezhnoho nadannia publichnykh posluh u zviazku zi zminamy administratyvno-terrytorialnoho ustrou Ukrainy [On risks in providing an appropriate level of public services related to changes in administrative and territorial structure of Ukraine]. Kyiv: NISS. Retrieved from https://niss.gov.ua/sites/default/files/2020-10/publichni-poslugy-1.pdf [in Ukrainian].

Kramer, F. D., Binnendijk, H., & Hamilton, D. (2015). Defend the Arteries of Society. *US News and World Report*. Retrieved from http://www.usnews.com/opinion/blogs/world-report/2015/06/09/russia-ukraine-and-the-rise-of-hybrid-warfare

Lasconjarias, G. (2017). Deterrence through Resilience. NATO, the Nations and the Challenges of Being Prepared. Research Division – NATO Defense College, Rome. *Eisenhower Paper, 7,* 1–8.

Law of Ukraine. (1991). Pro Zbroini Syly Ukrainy [On the Armed Forces of Ukraine]. *Vidomosti Verkhovnoi Rady Ukrainy, 9*, art. 108. [in Ukrainian].

Law of Ukraine. (1992). Pro oboronu Ukrainy [On the Defense of Ukraine]. *Vidomosti Verkhovnoi Rady Ukrainy, 9,* 106. [in Ukrainian].

Law of Ukraine. (1996). Konstytutsiia Ukrainy [Constitution of Ukraine]. *Vidomosti Verkhovnoi Rady Ukrainy, 30,* art. 141. [in Ukrainian].

Law of Ukraine. (1998). Pro Radu natsionalnoi bezpeky i oborony Ukrainy [On the National Defense and Security Council of Ukraine]. *Vidomosti Verkhovnoi Rady Ukrainy, 35,* art. 237. [in Ukrainian].

Law of Ukraine. (2003a). Pro borotbu z teroryzmom [On combating terrorism]. *Vidomosti Verkhovnoi Rady Ukrainy, 25,* art. 180. [in Ukrainian].

Law of Ukraine. (2003b). Pro osnovy natsionalnoi bezpeky Ukrainy [On the Foundations of the National Security of Ukraine]. *Vidomosti Verkhovnoi*

Rady Ukrainy, 19, art. 351. [in Ukrainian].

Law of Ukraine. (2005). Pro orhanizatsiiu oboronnoho planuvannia [On the Defense Planning]. *Vidomosti Verkhovnoi Rady Ukrainy, 4,* art. 97. [in Ukrainian].

Law of Ukraine. (2006). Pro Derzhavnu sluzhbu spetsialnoho zviazku ta zakhystu informatsii Ukrainy [On the State Special Communication and Information Protection Service of Ukraine]. *Vidomosti Verkhovnoi Rady* Ukrainy, 30, art. 258. [in Ukrainian].

Law of Ukraine. (2010). Pro derzhavno-pryvatne partnerstvo [On State-Private Partnership]. *Vidomosti Verkhovnoi Rady Ukrainy, 40,* art. 524. [in Ukrainian].

Law of Ukraine. (2011). Pro volontersku diialnist [On Volunteer Activities]. *Vidomosti Verkhovnoi Rady Ukrainy*, *42*, art. 435. [in Ukrainian].

Law of Ukraine. (2012). Pro systemu ekstrenoi dopomohy naselenniu za yedynym telefonnym nomerom 112 [On the Emergency Aid to the Population Using Single Phone Number 112]. *Vidomosti Verkhovnoi Rady Ukrainy*, *49*, art. 560. [in Ukrainian].

Law of Ukraine. (2013a). Kodeks tsyvilnoho zakhystu Ukrainy [Code of Civil Protection of Ukraine]. *Vidomosti Verkhovnoi Rady Ukrainy*, *34-35*, art. 458. [in Ukrainian].

Law of Ukraine. (2013b). Pro ekstrenu medychnu dopomohu [On Emergency Medical Care]. *Vidomosti Verkhovnoi Rady Ukrainy, 30,* art. 340. [in Ukrainian].

Law of Ukraine. (2014). Pro spivrobitnytstvo terytorialnykh hromad [On Cooperation between territorial communities]. *Vidomosti Verkhovnoi Rady Ukrainy, 34*, art. 1167. [in Ukrainian].

Law of Ukraine. (2017). Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy [On the Foundations of the Cybersecurity in Ukraine]. *Vidomosti Verkhovnoi Rady Ukrainy, 45,* art. 403. [in Ukrainian].

Law of Ukraine. (2018). Pro natsionalnu bezpeku Ukrainy [On the National

Security of Ukraine]. *Vidomosti Verkhovnoi Rady Ukrainy, 31,* art. 241. [in Ukrainian].

Lee, A. V., Vargo, J., & Seville, E. (2013). Developing a Tool to Measure and Compare Organizations` Resilience. *Natural Hazards Review, 14,* 29–41.

Legislation of Ukraine. (2003). *Pro zatverdzhennia Polozhennia pro korabelnu sluzhbu u Viiskovo-Morskykh Sylakh Zbroinykh Syl Ukrainy* [On approving the Regulation on the sea duty with the Navy of the Armed Forces of Ukraine]. Order of the Ministry of Defense of Ukraine No 415. Retrieved from https://zakon.rada.gov.ua/laws/show/z1170-03#Text [in Ukrainian].

Legislation of Ukraine. (2004). *Pro zatverdzhennia Instruktsii z borotby za zhyvuchist suden vnutrishnoho plavannia* [On approving the Instruction on Ship Damage Control Procedures for Inland vessels]. Order of the Ministry of Transportation and Communications of Ukraine No 963. Retrieved from https://zakon.rada.gov.ua/laws/show/z1483-04#Text [in Ukrainian].

Legislation of Ukraine. (2011). *Pro zatverdzhennia Vymoh do vyznachennia poriadku dii personalu pidrozdilu fizychnoho zakhystu, personalu pidrozdilu obliku ta kontroliu yadernykh materialiv v umovakh nadzvychainykh i kryzovykh sytuatsii* [On approving Requirements to operating procedures for the physical protection unit personnel, nuclear materials accounting, and control unit personnel during emergencies and crises]. Order of the Ministry of Energy and Coal Industry of Ukraine and the Ministry of Emergencies of Ukraine No 501/1001. Retrieved from https://zakon.rada.gov.ua/laws/show/z1147-11#Text [in Ukrainian].

Legislation of Ukraine. (2015). *Pro zatverdzhennia Pravyl aviatsiinoho poshuku i riatuvannia v Ukraini* [On approving the Rules for aviation search and rescue in Ukraine]. Order of the Ministry of Internal Affairs of Ukraine No 279. Retrieved from https://zakon.rada.gov.ua/laws/show/z0364-15#Text [in Ukrainian].

Legislation of Ukraine. (2017a). *Pro zatverdzhennia Instruktsii z provedennia analizu ryzykiv u Derzhavnii prykordonnii sluzhbi Ukrainy* [On approving the Instruction on risk analysis in the State Border Guard Control Service of Ukraine]. Order of the Ministry of Internal Affairs of Ukraine No 1007. Retrieved from https://zakon.rada.gov.ua/laws/show/z0091-18#Text [in Ukrainian].

Legislation of Ukraine. (2017b). *Pro zatverdzhennia Pravyl okhorony pratsi pid chas vykonannia sudnobudivnykh ta sudnoremontnykh robit* [On approving the work safety rules during shipbuilding and ship repair operations]. Order of the Ministry of Social Policy of Ukraine No 1491. Retrieved from https://zakon.rada.gov.ua/laws/show/z1291-17#Text [in Ukrainian].

Legislation of Ukraine. (2018a). *Pro zatverdzhennia Kodeksu systemy peredachi* [On approving the Code on power transfer system]. Resolution of the National commission that performs national regulation in energy and utilities sphere No 309. Retrieved from https://zakon.rada.gov.ua/laws/show/v0309874-18#Text [in Ukrainian].

Legislation of Ukraine. (2018b). *Pro zatverdzhennia Poriadku zarakhuvannia, vidrakhuvannia ta perevedennia uchniv do derzhavnykh ta komunalnykh zakladiv osvity dlia zdobuttia povnoi zahalnoi serednoi osvity* [On approving the Procedures on enrolling, expelling and transferring students to/from national and community education establishments in order to obtain complete general secondary education]. Order of the Ministry of education and science of Ukraine No 367. Retrieved from https://zakon.rada.gov.ua/laws/show/z0564-18#Text [in Ukrainian].

Legislation of Ukraine. (2020a). *Pro vstanovlennia vymoh z bezpeky ta zakhystu informatsii do kvalifikovanykh nadavachiv elektronnykh dovirchykh posluh ta yikhnikh vidokremlenykh punktiv reiestratsii* [On establishing security and information assurance requirements for the qualified electronic confidential services providers and their distributed registration points]. Order of the Administration of the State Special Communications and Information Protection Service of Ukraine No 269. Retrieved from https://zakon.rada.gov.ua/laws/show/z0668-20#Text [in Ukrainian].

Legislation of Ukraine. (2020b). *Pro zatverdzhennia normatyvno-pravovykh aktiv z pytan nadannia ekstrenoi medychnoi dopomohy* [On approving legislation in the area of providing emergency medical aid]. Order of the Ministry of Health of Ukraine No 2179. Retrieved from https://zakon.rada.gov.ua/laws/show/z1192-20#Text [in Ukrainian].

Lentzos, F. & Rose, N. (2009). Governing insecurity: Contingency planning, protection, resilience. *Economy and Society*, *38(2),* 230–254.

Lewes, G. H. (1875). *Problems of Life and Mind. First Series: The Foundations of a Creed.* Vol. II. Boston: Osgood. Retrieved from https://books.google.com.ua/books?id=0J8RAAAAYAAJ&redir_esc=y

Libanova, E. M. (2020). *Bidnist naselennia Ukrainy: metodolohiia, metodyka ta praktyka analizu* [Powerty of the population of Ukraine: analysis methodology, tools, and practice]. Uman: vydavets Sochynskyi M.M. [in Ukrainian].

Lyon, C. (2014). Place systems and social resilience: a framework for understanding place in social adaptation, resilience, and transformation. *Society & Natural Resources, 27,* 1009–1023. Retrieved from https://www.tandfonline.com/doi/abs/10.1080/08941920.2014.918228

Magis, K. (2010). Community resilience: an indicator of social sustainability. *Society & Natural Resources, 23,* 401–416. Retrieved from https://www.tandfonline.com/doi/abs/10.1080/08941920903305674

Martin-Breen, P., & Anderies, J. M. (2011). *Resilience: A Literature Review*. Bellagio Initiative. Retrieved from https://opendocs.ids.ac.uk/opendocs/bitstream/handle/123456789/3692/Bellagio-Rockefeller%20bp.pdf?sequence=1&isAllowed=y

Meadows, D.H., Randers, J., & Medows, D.L. (2012). *Predely rosta: 30 let spustia* [The limits to growth]. Moscow: BINOM. [in Russian].

Miller, F., Osbahr, H., Boyd, E., Thomalla, F., Bharwani, S., Ziervogel, G., …Nelson, D. (2010). Resilience and vulnerability: complementary or conflicting concepts? *Ecology and Society*, *15(3),* art. 11. Retrieved from https://www.ecologyandsociety.org/vol15/iss3/art11/

Mitchell, M., Griffith, R., Ryan, P., Walkerden, G., Walker, B., Brown, V. A., Robinson, S. (2014). Applying resilience thinking to natural resource management through a "planning-by-doing" framework. *Society & Natural Resources, 27,* 299–314. Retrieved from https://www.researchgate.net/publication/260418608_Applying_Resilience_Thinking_to_Natural_Resource_Management_through_a_Planning-By-Doing_Framework

Moench, M., & Dixit, A. (Eds.). (2007). *Working with the winds of change: towards strategies for responding to the risks associated with climate change and other hazards.* ProVention Consortium; Institute for Social and Environmental Transition-International; Institute for Social and Environmental Transition-Nepal. Kathmandu: Format Printing Press. Retrieved from https://www.unisdr.org/files/2652_windsofchange.pdf

National Security Authority of the Slovak Republic. (2018). Koncepcia pre boj Slovenskej Republiky proti hybridnym hrozbam [Concept of the Slovak Republic to combat hybrid threats]. Retrieved from https://www.nbu.gov.sk/wp-content/uploads/PHHD/Koncepcia-boja-SR-proti-hybridnym-hrozbam.pdf [in Slovak].

National Resilience Promotion Office of the Cabinet Secretariat of Japan. (n.d.). Building National Resilience. Creating a Strong and Flexible Country. Retrieved from https://www.cas.go.jp/jp/seisaku/kokudo_kyoujinka/en/e01_panf.pdf

NATO. (1949). *North-Atlantic Treaty.* Washington, D.C., 4 April 1949 (in Ukrainian/ Russian). Retrieved from https://zakon.rada.gov.ua/laws/show/950_008#Text

NATO. (2001). *NATO's Role in Disaster Assistance.* Second Edition. NATO. Retrieved from https://www.nato.int/eadrcc/mcda-e.pdf

NATO. (2014). *Wales Summit Declaration*. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in

Wales. Retrieved from https://www.nato.int/cps/en/natohq/official_texts_112964.htm

NATO. (2016a). *Allies move forward on enhancing NATO's resilience*. Retrieved from https://www.nato.int/cps/en/natohq/news_135288.htm?selectedLocale=en

NATO. (2016b). *Commitment to enhance resilience.* Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw, 8–9 July 2016. Retrieved from https://www.nato.int/cps/su/natohq/official_texts_133180.htm

NATO. (2016c). *Warsaw Summit Communiqué*. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw. Retrieved from https://www.nato.int/cps/en/natohq/official_texts_133169.htm

NATO. (2021a). *Brussels Summit Communiqué*. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 14 June 2021. Retrieved from https://www.nato.int/cps/en/natohq/news_185000.htm

NATO. (2021b). *Civil preparedness.* Retrieved from https://www.nato.int/cps/en/natohq/topics_49158.htm

NATO. (2021c). *On the Agenda.* Brussels Summit, 14 June 2021. Retrieved from https://www.nato.int/cps/en/natohq/news_184633.htm?selectedLocale=en#3

NATO. (2021d). *Resilience and Article 3.* Retrieved from https://www.nato.int/cps/fr/natohq/topics_132722.htm?selectedLocale=en

NATO. (2021e). *Strengthened Resilience Commitment*. Retrieved from https://www.nato.int/cps/en/natohq/official_texts_185340.htm

New Zealand Department of the Prime Minister and Cabinet. (2016). *National Security System. Handbook.* Retrieved from https://dpmc.govt.nz/sites/default/files/2017-03/dpmc-nss-handbook-aug-2016.pdf

New Zealand Department of the Prime Minister and Cabinet. (2019). *Annual* *report 2018/2019*. Retrieved from https://dpmc.govt.nz/sites/default/files/2019-10/dpmc-annual-report-2019.pdf

New Zealand Department of the Prime Minister and Cabinet. (2020a). *Annual report 2019/2020*. Retrieved from https://www.civildefence.govt.nz/assets/Uploads/publications/dpmc-annual-report-2020.pdf

New Zealand Department of the Prime Minister and Cabinet. (2020b). *National Assessments Bureau*. Retrieved from https://dpmc.govt.nz/our-business-units/national-security-group/national-assessments-bureau

New Zealand Department of the Prime Minister and Cabinet. (2021a). *National Risk Approach*. Retrieved from https://dpmc.govt.nz/our-programmes/national-security/national-risk-approach-0

New Zealand Department of the Prime Minister and Cabinet. (2021b). *National Security and Intelligence Priorities*. Retrieved from https://dpmc.govt.nz/our-programmes/national-security-and-intelligence/national-security-and-intelligence-priorities

New Zealand Department of the Prime Minister and Cabinet. (2021c). *National Security Group*. Retrieved from https://dpmc.govt.nz/our-business-units/national-security-group

New Zealand Government. (2019a). Coordinated Incident Management System. 3rd edition. Retrieved from https://www.civildefence.govt.nz/assets/Uploads/CIMS-3rd-edition-FINAL-Aug-2019.pdf

New Zealand Government. (2019b). National Disaster Resilience Strategy 2019. Retrieved from https://www.civildefence.govt.nz/assets/Uploads/publications/National-Disaster-Resilience-Strategy/National-Disaster-Resilience-Strategy-10-April-2019.pdf

New Zealand Legislation. (2002). *Civil Defence Emergency Management Act*. NZ

Public Act No 33. Retrieved from https://www.legislation.govt.nz/act/public/2002/0033/51.0/DLM149789.html

New Zealand Legislation. (2015). National Civil Defence Emergency Management Plan Order 2015. Retrieved from https://www.legislation.govt.nz/regulation/public/2015/0140/latest/whole.htmlNo. DLM6486658

New Zealand Standards. (2009). *Risk management – Principles and guidelines.* AS/NZS ISO 31000:2009. Retrieved from https://www.standards.govt.nz/shop/asnzs-iso-310002009/

National Institute for Strategic Studies [NISS]. (2020). *Analitychna dopovid do shchorichnoho Poslannia Prezydenta Ukrainy do Verkhovnoi Rady Ukrainy «Pro vnutrishnie ta zovnishnie stanovyshche Ukrainy»* [Analytical report to the annual address of the President of Ukraine to the Verkhovna Rada of Ukraine "On domestic and foreign situation of Ukraine"]. Retrieved from https://niss.gov.ua/publikacii/poslannya-prezidenta-ukraini/analitichna-dopovid-do-schorichnogo-poslannya-prezidenta-4 [in Ukrainian].

Norris, F. H., Stevens, S. P., Pfefferbaum, B., Wyche, K. F., & Pfefferbaum, R. L. (2008). Community Resilience as a Metaphor. Theory. Set of Capacities and Strategy for Disaster Readiness. *American Journal of Community Psychology, 41(1-2),* 127–150.

Norwegian Ministry of Defence, Norwegian Ministry of Justice and Public Security. (2018). *Support and Cooperation.* A description of the total defence in Norway. Retrieved from https://www.regjeringen.no/contentassets/5a9bd774183b4d548e33da101e7f7d43/support-and-cooperation.pdf

Nyzhnyk, N.R., Sytnyk, H.P., & Bilous, V.T. (2000). Natsionalna bezpeka Ukrainy (metodolohichni aspekty, stan i tendentsii rozvytku) [National security of Ukraine (methodology aspects, status and development trends)]. Irpin: Presa Ukrainy.

OECD. (n.d.a). *National policy frameworks on resilience in OECD countries.*

Retrieved from http://www.oecd.org/cfe/regional-policy/national-policy-resilience-frameworks.pdf

OECD. (n.d.b). *Resilience Systems Analysis.* Learning & Recommendations report. Retrieved from https://www.oecd.org/dac/conflict-fragility-resilience/docs/SwedenLearning_Recommendationsreport.pdf

OECD. (n.d.c). *Risk and Resilience.* Retrieved from https://www.oecd.org/dac/conflict-fragility-resilience/risk-resilience/

OECD. (2002). Glossary of Key Terms in Evaluation and Results Based Management. *Evaluation and Aid Effectiveness, No 6.* Paris. Retrieved from https://www.oecd.org/dac/31650813.pdf

OECD. (2008). Concepts and Dilemmas of State Building in Fragile Situations: From Fragility to Resilience. *OECD/DAC Discussion Paper*. Retrieved from https://www.oecd.org/dac/conflict-fragility-resilience/docs/41100930.pdf

OECD. (2013). *What does "resilience" mean for donors?* An OECD factsheet. Retrieved from https://www.oecd.org/dac/May%2010%202013%20FINAL%20resilience%20PDF.pdf

OECD. (2014a). *Guidelines for Resilience Systems Analysis*. Strasbourg : OECD Publishing. Retrieved from https://www.oecd.org/dac/conflict-fragility-resilience/Resilience%20Systems%20Analysis%20FINAL.pdf

OECD. (2014b). *Overview Paper on Resilient Economies and Societies.* Meeting of the OECD Council at Ministerial Level. Retrieved from https://www.oecd.org/mcm/C-MIN(2014)7-ENG.pdf

OECD. (2016). *Resilient Cities.* Policy Highlights of the OECD Report (Preliminary version). Retrieved from https://www.mlit.go.jp/common/001136418.pdf

OECD. (2017). *National Risk Assessment: A Cross Country Perspective.* Paris: OECD Publishing. Retrieved from http://dx.doi.org/10.1787/9789264287532-en

Office of the Prime Minister of Finland. (2017). *Minister for Foreign Affairs of*

Finland Mr Timo Soini at the signing of the Memorandum of Understanding establishing the European Centre of Excellence for Countering Hybrid Threats. Helsinki. Retrieved from https://vnk.fi/documents/10616/3934867/Soini+on+hybrid+threats+11+April+clean+UMIK.pdf

Office of the Prime Minister of Japan. (2013). *National Security Strategy*. (Provisional translation). Retrieved from http://japan.kantei.go.jp/96_abe/documents/2013/_icsFiles/afieldfile/2013/12/17/NSS.pdf

OSCE. (n.d.). *Disaster Risk Reduction*. Retrieved from https://www.osce.org/oceea/disaster-risk-reduction

OSCE. (2014). *Preventing Terrorism and Countering Violent Extremism and Radicalization that Lead to Terrorism: A Community-Policing Approach*. Retrieved from https://www.osce.org/secretariat/111438?download=true

OSCE. (2015). *Povernennia do dyplomatii* [Back to Diplomacy]. Final Report and Recommendations of the Panel of Eminent Persons on European Security as a Common Project. Retrieved from https://www.osce.org/files/f/documents/e/6/265421.pdf [in Ukrainian]

OSCE. (2017). *Strengthening resilience of local communities to the presence of migrants*. Retrieved from https://www.osce.org/secretariat/323471

OSCE. (2020). *Improve transparency and institutions` resilience in fight against corruption urge participants of 2020 OSCE Forum in Prague*. Retrieved from https://www.osce.org/chairmanship/463236

Ovchinnikov, N.F. (1969). Struktura i simmetriia [Structure and symmetry]. In *Systemnye issledovaniia: ezhegodnik* [Systemic research: annual periodical] (pp. 111–121). Moscow: Nauka. [in Russian].

Parsons, T. (1977). *Social Systems and the Evolution of Action Theory*. New York: Free Press.

Pfefferbaum, B., Reissman, D., Pfefferbaum, R., Klomp, R., & Gurwitch R. (2007). Building resilience to mass trauma events. In L. Doll, S. Bonzo, D.

Sleet, J. Mercy (Eds.). *Handbook on Injury and Violence Prevention* (pp. 347–358). Springer.

Polasky, S., Carpenter, S. R., Folke, C., & Keeler, B. (2011). Decision-making under great uncertainty: environmental management in an era of global change. *Trends in Ecology and Evolution, 26,* 398–404. Retrieved from https://www.researchgate.net/publication/51168974_Decision-making_under_great_uncertainty_Environmental_management_in_an_era_of_global_change

Pollack, J. H., & Wood, J. D. (2010). *Enhancing Public Resilience to Mass-Casualty WMD Terrorism in the United States: Definitions, Challenges, and Recommendations.* Defense Threat Reduction Agency, Advanced Systems and Concepts Office. Retrieved from https://fas.org/irp/agency/dod/dtra/resilience.pdf

President of the Russian Federation. (2021). *O Strategii natcionalnoi bezopasnosti Rossiiskoi Federatcii* [On National Security Strategy of the Russian federation]. Decree President of the Russian Federation No 400. Retrieved from http://publication.pravo.gov.ru/Document/View/0001202107030001?index=0&rangeSize=1 [in Russian].

President of the United States of America. (2017). National Security Strategy of the United States of America. Retrieved from https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

President of Ukraine. (2006). *Pro Polozhennia pro poriadok pidhotovky ta vnesennia proektiv aktiv Prezydenta Ukrainy* [On the Regulation on drafting and submitting draft acts of the President of Ukraine]. Decree of the President of Ukraine, No 970/2006. Retrieved from https://zakon.rada.gov.ua/laws/show/970/2006#Text [in Ukrainian].

President of Ukraine. (2007). *Pro Stratehiiu natsionalnoi bezpeky Ukrainy* [On the National Security Strategy of Ukraine]. Decree of the President of Ukraine, No 105/2007. Retrieved from http://zakon0.rada.gov.ua/laws/show/105/2007/ed20070212 [in Ukrainian].

President of Ukraine. (2012). *Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 8 chervnia 2012 roku «Pro novu redaktsiiu Stratehii natsionalnoi bezpeky Ukrainy»* [On the decision of the National Defense and Security Council of Ukraine dated June 8, 2012 “On the new release of the National Security Strategy of Ukraine”]. Decree of the President of Ukraine, No 389/2012. Retrieved from http://zakon0.rada.gov.ua/laws/show/389/2012/paran18#n18 [in Ukrainian].

President of Ukraine. (2015a). *Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 25 sichnia 2015 roku "Pro stvorennia ta zabezpechennia diialnosti Holovnoho sytuatsiinoho tsentru Ukrainy"* [On the decision of the National Defense and Security Council of Ukraine dated January 25, 2015 “On Establishing and Supporting the Main Situational Center of Ukraine”]. Decree of the President of Ukraine, No 115/2015. Retrieved from https://zakon.rada.gov.ua/laws/show/115/2015#n2 [in Ukrainian].

President of Ukraine. (2015b). *Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 6 travnia 2015 roku "Pro Stratehiiu natsionalnoi bezpeky Ukrainy"* [On the decision of the National Defense and Security Council of Ukraine dated May 6, 2015 “On the National Security Strategy of Ukraine”]. Decree of the President of Ukraine, No 287/2015. Retrieved from http://zakon2.rada.gov.ua/laws/show/287/2015 [in Ukrainian].

President of Ukraine. (2015c). *Pro Stratehiiu staloho rozvytku "Ukraina - 2020"* [On the Sustained Development Strategy “Ukraine-2020”]. Decree of the President of Ukraine, No 5/2015. Retrieved from https://zakon.rada.gov.ua/laws/show/5/2015#Text [in Ukrainian].

President of Ukraine. (2015d). *Pro zatverdzhennia Richnoi natsionalnoi prohramy spivrobitnytstva Ukraina - NATO na 2015 rik* [On approving the Ukraine-NATO Annual National Program for 2015]. Decree of the President of Ukraine, No 238/2015. Retrieved from https://zakon.rada.gov.ua/laws/show/238/2015#Text [in Ukrainian].

President of Ukraine. (2016a). *Pro Natsionalnyi koordynatsiinyi tsentr kiberbezpeky* [On the National Cybersecurity coordination center]. Decree of the President of Ukraine, No 242/2016. Retrieved from https://zakon.rada.gov.ua/laws/show/242/2016#Text [in Ukrainian].

President of Ukraine. (2016b). *Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 27 sichnia 2016 roku "Pro Stratehiiu kiberbezpeky Ukrainy"* [On the decision of the National Defense and Security Council of Ukraine dated January 27, 2016 “On the Cybersecurity Strategy of Ukraine”]. Decree of the President of Ukraine, No 96/2016. Retrieved from https://zakon.rada.gov.ua/laws/show/96/2016#n11 [in Ukrainian].

President of Ukraine. (2019a). *Pro Kontseptsiiu borotby z teroryzmom v Ukraini* [On the Countering terrorism concept]. Decree of the President of Ukraine, No 53/2019. Retrieved from https://zakon.rada.gov.ua/laws/show/53/2019#Text [in Ukrainian].

President of Ukraine. (2019b). *Pro Poriadok provedennia ohliadu zahalnoderzhavnoi systemy borotby z teroryzmom* [On the Procedures to review the national system for countering terrorism]. Decree of the President of Ukraine, No 506/2019. Retrieved from https://zakon.rada.gov.ua/laws/show/506/2019#Text [in Ukrainian].

President of Ukraine. (2019c). *Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 16 travnia 2019 roku "Pro orhanizatsiiu planuvannia v sektori bezpeky i oborony Ukrainy"* [On the decision of the National Defense and Security Council of Ukraine dated May 16, 2019 “On Planning in the Security and Defense Sector of Ukraine”]. Decree of the President of Ukraine, No 225/2019. Retrieved from https://zakon.rada.gov.ua/laws/show/225/2019#Text [in Ukrainian].

President of Ukraine. (2019d). *Pytannia Komisii z pytan koordynatsii yevroatlantychnoi intehratsii Ukrainy* [Issues of the Board on Coordinating Euro-Atlantic integration of Ukraine]. Decree of the President of Ukraine, No. 784/2019. Retrieved from https://zakon.rada.gov.ua/laws/show/784/2019#Text

President of Ukraine. (2019e). *Pro Tsili staloho rozvytku Ukrainy na period do 2030 roku* [On the Goals of the Sustained Development of Ukraine until 2030]. Decree of the President of Ukraine, No 722/2019. Retrieved from https://zakon.rada.gov.ua/laws/show/722/2019#Text [in Ukrainian].

President of Ukraine. (2020a). *Pro Richnu natsionalnu prohramu pid ehidoiu Komisii Ukraina - NATO na 2020 rik* [On the Annual National Program under the auspices of the Ukraine-NATO Commission for 2020]. Decree of the President of Ukraine, No 203/2020. Retrieved from https://zakon.rada.gov.ua/laws/show/203/2020#Text [in Ukrainian].

President of Ukraine. (2020b). *Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 veresnia 2020 roku "Pro Stratehiiu natsionalnoi bezpeky Ukrainy"* [On the decision of the National Defense and Security Council of Ukraine dated September 14, 2020 “On the National Security Strategy of Ukraine”]. Decree of the President of Ukraine, No 392/2020. Retrieved from https://zakon.rada.gov.ua/laws/show/392/2020#Text [in Ukrainian].

President of Ukraine. (2020c). *Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 24 bereznia 2020 roku "Pro zvit shchodo rezultativ provedennia oboronnoho ohliadu Ministerstvom oborony Ukrainy"* [On the decision of the National Defense and Security Council of Ukraine dated March 24, 2020 “On the Report on Results of the Defense Review by the Ministry of Defense of Ukraine”]. Decree of the President of Ukraine, No 106/2020. Retrieved from https://zakon.rada.gov.ua/laws/show/106/2020 [in Ukrainian].

President of Ukraine. (2020d). *Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 29 hrudnia 2020 roku "Pro rezultaty provedennia ohliadu hromadskoi bezpeky ta tsyvilnoho zakhystu"* [On the decision of the National Defense and Security Council of Ukraine dated December 29, 2020 “On Results of the Review of Public Security and Civil Defense”].

Decree of the President of Ukraine, No 597/2020. Retrieved from https://zakon.rada.gov.ua/laws/show/597/2020#Text [in Ukrainian].

President of Ukraine. (2021a). *Pro Richnu natsionalnu prohramu pid ehidoiu Komisii Ukraina - NATO na 2021 rik* [On the Annual National Program under the auspices of the Ukraine-NATO Commission for 2021]. Decree of the President of Ukraine, No 189/2021. Retrieved from https://zakon.rada.gov.ua/laws/show/189/2021#Text [in Ukrainian].

President of Ukraine. (2021b). *Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 11 serpnia 2021 roku "Pro Stratehiiu ekonomichnoi bezpeky Ukrainy na period do 2025 roku"* [On the decision of the National Defense and Security Council of Ukraine dated August 11, 2021 “On the Economic Security Strategy until 2025”]. Decree of the President of Ukraine, No 347/2021. Retrieved from https://zakon.rada.gov.ua/laws/show/347/2021#n2 [in Ukrainian].

President of Ukraine. (2021c). *Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku "Pro Stratehiiu kiberbezpeky Ukrainy"* [On the decision of the National Defense and Security Council of Ukraine dated May 14, 2021 “On the Cybersecurity Strategy of Ukraine”]. Decree of the President of Ukraine, No 447/2021. Retrieved from https://www.president.gov.ua/documents/4472021-40013 [in Ukrainian].

President of Ukraine. (2021d). *Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku "Pro Stratehiiu liudskoho rozvytku"* [On the decision of the National Defense and Security Council of Ukraine dated May 14, 2021 “On the Human Development Strategy”]. Decree of the President of Ukraine, No 225/2021. Retrieved from https://zakon.rada.gov.ua/laws/show/225/2021#n2 [in Ukrainian].

President of Ukraine. (2021e). *Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 15 kvitnia 2021 roku "Pro rezultaty provedennia ohliadu oboronno-promyslovoho kompleksu"* [On the decision of the National Defense and Security Council of Ukraine dated April 15, 2021 “On results of the Defense Industrial Complex Review”]. Decree of the President of Ukraine, No 168/2021. Retrieved from https://zakon.rada.gov.ua/laws/show/168/2021#Text [in Ukrainian].

President of Ukraine. (2021f). *Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 18 chervnia 2021 roku «Pro Stratehiiu rozvytku oboronno-promyslovoho kompleksu Ukrainy»* [On the decision of the National Defense and Security Council of Ukraine dated June 18, 2021 “On the Strategy for the Development of the Defense Industrial Complex of Ukraine”]. Decree of the President of Ukraine, No 372/2021. Retrieved from https://www.president.gov.ua/documents/3722021-39733 [in Ukrainian].

President of Ukraine. (2021g). Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 20 serpnia 2021 roku «Pro zaprovadzhennia natsionalnoi systemy stiikosti» [On the Decision of the National Security and Defense Council of Ukraine of August 20, 2021 “On the Introduction of the National Resilience System”]. Decree of the President of Ukraine, No 479/2021. Retrieved from https://www.president.gov.ua/documents/4792021-40181 [in Ukrainian].

President of Ukraine. (2021h). *Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 23 bereznia 2021 roku "Pro rezultaty provedennia ohliadu rozviduvalnykh orhaniv Ukrainy"* [On the decision of the National Defense and Security Council of Ukraine dated March 23, 2021 “On the Results of the Review of the Intelligence Organizations of Ukraine”]. Decree of the President of Ukraine, No 110/2021. Retrieved from https://zakon.rada.gov.ua/laws/show/110/2021#Text [in Ukrainian].

President of Ukraine. (2021i). *Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 25 bereznia 2021 roku "Pro Stratehiiu voiennoi bezpeky Ukrainy"* [On the decision of the National Defense and Security Council of Ukraine dated March 25, 2021 “On the Military Security Strategy of Ukraine”]. Decree of the President of Ukraine, No 121/2021. Retrieved from https://zakon.rada.gov.ua/laws/show/121/2021#Text [in Ukrainian].

President of Ukraine. (2021j). *Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 30 lypnia 2021 roku "Pro Stratehiiu zovnishnopolitychnoi diialnosti Ukrainy"* [On the decision of the National Defense and Security Council of Ukraine dated July 30, 2021 "On Foreign Policy Strategy of Ukraine"]. Decree of the President of Ukraine, No 448/2021. Retrieved from https://www.president.gov.ua/documents/4482021-40017 [in Ukrainian].

President of Ukraine. (2021k). *Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 4 chervnia 2021 roku "Pro zvit shchodo rezultativ provedennia ohliadu zahalnoderzhavnoi systemy borotby z teroryzmom"* [On the decision of the National Defense and Security Council of Ukraine dated June 4, 2021 "On the Report of the Results of Review of the National Countering Terrorism System"]. Decree of the President of Ukraine, No 251/2021. Retrieved from https://zakon.rada.gov.ua/laws/show/251/2021#Text [in Ukrainian].

President of Ukraine. (2021l). *Pro zatverdzhennia Polozhennia pro Konhres mistsevykh ta rehionalnykh vlad pry Prezydentovi Ukrainy* [On approving the Regulation on the Congress of local and regional authorities under the President of Ukraine]. Decree of the President of Ukraine, No 89/2021. Retrieved from https://zakon.rada.gov.ua/laws/show/89/2021#Text [in Ukrainian].

President of Ukraine. (2021m). *Prezydent zatverdyv plan dopusku inozemnykh viiskovykh v Ukrainu dlia provedennia navchan u 2021 rotsi* [The President has approved the plan to allow access for the foreign military to Ukraine to conduct exercises in 2021]. Retrieved from https://www.president.gov.ua/news/prezident-zatverdiv-plan-dopusku-inozemnih-vijskovih-v-ukray-66413 [in Ukrainian].

Prigozhyn, I., & Stengers, J. (1986). *Poriadok iz khaosa: novyi dialog cheloveka s prirodoy* [Order from chaos: new dialog between a human being and nature]. Moscow: Progress. [in Russian]

Prior, T., & Hagmann, J. (2012). *Measuring Resilience: Benefits and Limitations of Resilience Indices.* SKI Focus Report 8. Center for Security Studies (CSS). Zurich: ETH. Retrieved from https://www.files.ethz.ch/isn/173644/Focal-Report_-8-Measuring_Resilience_2013.pdf

Proag, V. (2014). The concept of vulnerability and resilience. *Building Resilience 2014: 4th International Conference on Building Resilience (8–10 September 2014, Salford Quays, UK). Procedia Economics and Finance, 18,* 369–376.

Pursiainen, C., & Rød, B. (Eds.). (2016). Report of criteria for evaluating resilience. In *Improved risk evaluation and implementation of resilience concepts to Critical Infrastructure*. IMPROVER project. Retrieved from https://www.researchgate.net/publication/320286600_Report_of_criteria_for_evaluating_resilience

Rácz, A. (2015). *Russia's Hybrid War in Ukraine. Breaking the Enemy's Ability to Resist.* Finnish Institute of International Affairs.

Rapoport, A. (1969). Razlichnye podkhody k obschey teorii system [Various approaches to generic theory of systems]. In *Systemnye issledovaniia: ezhegodnik* [Systemic research: annual periodical] (pp. 55–79). Moscow: Nauka. [in Russian].

Razumkov Center. (2017). Politychna kultura ta parlamentarizm v Ukraini: suchasnyi stan ta osnovni problemy. [Political culture and parliamentarism in Ukraine: current status and basic issues]. In *Expert discussion on December 14, 2017, Information and analytical papers*. Retrieved from https://razumkov.org.ua/uploads/socio/2017_Politychna_kultura.pdf

Razumkov Center. (2018). Dovira hromadian do suspilnykh instytutiv. Resultaty sotsiolohichnoho doslidzhennia [Trust of the citizens to public institutions. Results of the sociological research]. Retrieved from https://razumkov.org.ua/uploads/socio/2018_06_press_release_ua.pdf

Razumkov Center. (2021). *Otsinka sytuatsii v kraini, dovira do instytutiv* *suspilstva ta politykiv, elektoralni orientatsii hromadian* [Assessment of the situation in the country, trust in public institutions and politicians, electoral orientation of the citizens]. Retrieved from https://razumkov.org.ua/napriamky/sotsiologichni-doslidzhennia/otsinka-sytuatsii-v-kraini-dovira-do-instytutiv-suspilstva-ta-politykiv-elektoralni-oriientatsii-gromadian-berezen-2021r

ReliefWeb. (2008). *Glossary of Humanitarian Terms.* Retrieved from https://reliefweb.int/sites/reliefweb.int/files/resources/4F99A3C28EC37D0EC12574A4002E89B4-reliefweb_aug2008.pdf

Rensel, D. J. (2015). Resilience – A Concept. *Defense ARJ, 22(3),* 294– 324.

Republic of Estonia Ministry of Defence. (2017). *National Security Concept.* Retrieved from https://kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_security_concept_2017.pdf

Resilience Alliance. (n.d.a). *Adaptive Management.* Retrieved from https://www.resalliance.org/adaptive-mgmt

Resilience Alliance. (n.d.b). *Glossary.* Retrieved from https://www.resalliance.org/glossary

Resilience Alliance. (2010). *Assessing resilience in social-ecological systems: Workbook for practitioners.* Version 2.0. Retrieved from https://www.resalliance.org/files/ResilienceAssessmentV2_2.pdf

Reznikova, O.O., & Driomov, S.V. (2016). Deyaki zakonodavchi aspekty protydii separatyzmu v Ukraini [legislative aspects of countering separatism in Ukraine]. *Stratehichni priorytety, 3,* 18–25. [in Ukrainian].

Reznikova, O.O., Misiura, A.O., Driomov, S.V., & Voytovskyi, K.Ye. (2017). *Aktualni pytannia protydii teroryzmu v sviti ta v Ukraini* [Key considerations for countering terrorism in the world and in Ukraine]. Kyiv: NISS. [in Ukrainian].

Reznikova, O.O., & Siomin, S.V. (2020). Problemy orhanizatsiynoho zabezpechennia rozbudovy natsionalnoi stiykosti v Ukraini [Problems of organizational support for building national resilience in Ukraine]. In *Public and municipal administration: theory, methodology, practice* (pp. 188–205). "VERN" University of Applied Sciences, Zagreb, Croatia. Riga: Izdevnieciba «Baltija Publishing». [in Ukrainian].

Reznikova, O.O., Tsiukalo, V.Yu., Palyvoda, V.O., Driomov, S.V., Siomin, S.V. (2015). *Kontseptualni zasady rozvytku systemy zabezpechennia natsionalnoi bezpeky Ukrainy* [Conceptual framework for development of the national security system of Ukraine]. Kyiv: NISS. Retrieved from https://niss.gov.ua/sites/default/files/2015-07/nac_bezp-182c8.pdf [in Ukrainian].

Reznikova, O.O., & Voytovskyi, K.Ye. (2020). *Schodo kontseptsii zabezpechennia natsionalnoi stiykosti v Ukraini* [On the concept of national resilience in Ukraine]. Kyiv: NISS. Retrieved from https://niss.gov.ua/sites/default/files/2021-02/analit-resnikova-national-security-8-2020-1-1.pdf [in Ukrainian].

Reznikova, O.O., & Voytovskyi, K.Ye. (2021). *Problema terminolohichnoi nevyznachenosti u sferi rozbudovy natsionalnoi stiykosti* [Issues of terminology ambiguity in the area of developing national resilience]. Kyiv: NISS. Retrieved from https://niss.gov.ua/sites/default/files/2021-01/az-7-gloss-060121_5.pdf [in Ukrainian].

Reznikova, O.O., Voytovskyi, K.Ye., & Lepikhov, A.V. (2020). *Natsionalni systemy otsinuvannia ryzykiv i zahroz: kraschi svitovi practyky, novi mozhlyvosti dlia Ukrainy* [National risks and threats assessment systems: best world practices, new opportunities for Ukraine]. Kyiv: NISS. [in Ukrainian].

Reznikova, O.O., Voytovskyi, K.Ye. & Lepikhov, A.V., (2021). *Organizatsiia systemy zabezpechennia natsionalnoi stiykosti na rehionalnomu i misttsevomu rivniakh* [Organization of the national resilience system at the regional and local levels]. Kyiv: NISS. [in Ukrainian].

Reznikova, O.O. (2013a). Problemy stiykosti Ukrainy do hlobalnykh ryzykiv:

ekonomichnyi aspekt [Issues of resilience of Ukraine to global risks: economic aspect]. *Stratehichni priority, 1,* 61–65. [in Ukrainian].

Reznikova, O.O. (2013b). Stiykist Ukrainy do hlobalnykh ryzykiv i problemy derzhavnoho upravlinnia [Resilience of Ukraine to global risks and issues of public administration]. *Stratehichni priorytety, 2,* 22–26. [in Ukrainian].

Reznikova, O.O. (2014). Perspektyvy hlobalnoho rozvytku u 2014 rotsi: vysnovky dlia Ukrainy [Future for the global development in 2014: conclusions for Ukraine]. *Stratehichni priorytety, 1,* 169–174. [in Ukrainian].

Reznikova, O.O. (2017). Zabezpechennia stiykosti derzhavy i suspilstva do terorystychnoi zahrozy v Ukraini ta sviti [Providing for the resilience of the state and society to terroristic threat in Ukraine and the world]. *Stratehichni priorytety, 3,* 22–28. [in Ukrainian].

Reznikova, O.O. (2018a). Formuvannia stiykosti derzhavy: vysnovky dlia Ukrainy [Building of the state resilience: conclusions for Ukraine]. *Visnyk Lvivskoho universitetu. Seriia: filosofsko-politlohichni studii, 20,* 193–199. [in Ukrainian].

Reznikova, O.O. (2018b). Kontseptualni zasady natsionalnoi stiykosti [Conceptual framework for national resilience]. *Derzhava i parvo, 81*, 135–146. [in Ukrainian].

Reznikova, O.O. (2018c). Mekhanizmy zabezpechennia stiykosti derzhavy u sferi natsionalnoi bezpeky [Tools for building the state resilience in the national security field]. *Stratehichni priorytety, 3-4*, 15–25. [in Ukrainian].

Reznikova, O.O. (2018d). Osoblyvosti formuvannia derzhavnoi polityky za pryntsypamy natsionalnoi stiykosti [Features of the state policy development based on the principles of national resilience]. *Visnyk Lvivskoho universitetu. Seriia: filosofsko-politlohichni studii*, *18*, 349–353. [in Ukrainian].

Reznikova, O.O. (2018e). Pasport separatystskoi zahrozy v Ukraini [Passport of the separatist threat in Ukraine]. *Stratehichni priorytety, 2,* 12–24. [in Ukrainian].

Reznikova, O.O. (2018f). Rozrobka stratehii natsionalnoi bezpeky z urakhuvanniam pryntsypiv natsionalnoi stiykosti [Developing a national security strategy based on the principles of national resilience]. *Stratehichna panorama, 2,* 5-11. [in Ukrainian].

Reznikova, O.O. (2018g). Zabezpechennia natsionalnoi bezpeky i natsionalnoi stiykosti: spilni rysy i vidminnosti [Providing for national security and national resilience: common features and differences]. *Visnyk Lvivskoho universitetu. Seriia: filosofsko-politlohichni studii, 19,* 170–175. [in Ukrainian].

Reznikova, O.O. (2019a). Formuvannia natsionalnoi stiykosti u konteksti implementatsii Ukrainou Tsiley staloho rozvytku [Building national resilience in the context of implementation of Sustainable development goals in Ukraine]. *Stratehichni priorytety, 2,* 27–37. [in Ukrainian].

Reznikova, O.O. (2019b). Kontseptualni pidkhody do rozrobky systemy rannioho poperedzhennia yak mekhanizmu zabezpechennia natsionalnoi stiykosti [Conceptual approaches to develop an early warning signal system as a mechanism for building national resilience]. *Visnyk Lvivskoho universitetu. Seriia: filosofsko-politlohichni studii*, *23*, 196–202. [in Ukrainian].

Reznikova, O.O. (2019c). Kontseptualni pidkhody do vyboru modeli zabezpechennia natsionalnoi stiykosti [Conceptual approaches to choice of the model for building national resilience]. *Stratehichni priorytety, 1*, 18–27. [in Ukrainian].

Reznikova, O.O. (2020a). Neobkhodimost politico-pravovykh transformatsiy v Ukraine dlia ukrepleniia natsionalnoy stoykosti [The necessity for political and legal transformations in Ukraine in order to strengthen national resilience]. In *Gesellschaftsrechtliche Transformationen von wirtschaftlichen Systemen in den Zeiten der Neo-Industrialisierung* (pp.626-635). Deutschland, Nurnberg: Verlag SWG imex GmbH. [in Russian].

Reznikova, O.O. (2020b). *On crisis management improvement and development of other national resilience components in the context of the COVID-19* *pandemia*. Kyiv: NISS. Retrieved from https://niss.gov.ua/sites/default/files/2020-04/reslience-covid-19.pdf

Reznikova, O.O. (2020c). *On the concept of national resilience in Ukraine*. Kyiv: NISS. Retrieved from https://niss.gov.ua/sites/default/files/2020-04/national-resilience_0.pdf

Reznikova, O.O. (2020d). Porivnialnyi analiz osnovnykh kontseptualnykh pidkhodiv do rozbudovy natsionalnoi stiykosti [Comparative analysis of the main conceptual approaches to building national resilience]. *Visnyk Lvivskoho universitetu. Seriia: filosofsko-politlohichni studii*, *28*, 175–181. [in Ukrainian].

Reznikova, O.O. (2020e). Problemy planuvannia u sferi natsionalnoi bezpeky Ukrainy [Problems of Implementation of the National Security Strategy of Ukraine]. *Stratehichna panorama, 1-2,* 5–13. [in Ukrainian].

Roepke, W.-D., & Thankey, H. (2019). *Resilience: the first line of defence*. NATO Review. Retrieved from https://www.nato.int/docu/review/articles/2019/02/27/resilience-the-first-line-of-defence/index.html

Rogers, P. (2013). Rethinking Resilience: Articulating Community and the UK Riots. *Politics, 33(4),* 322–333.

Rose, A. (2004). Defining and measuring economic resilience to disasters. *Disaster Prevention and Management, 13*, 307–314.

Rose, A. (2007). Economic Resilience to Natural and Man-Made Disasters: Multidisciplinary Origins and Contextual Dimensions. *Environmental Hazards, 7(4)*, 383–398

Rozumnyi, M.M. (2016). *Vyklyky natsionalnoho samovyznachennia* [Challenges of national self-determination]. Kyiv: National Institute for Strategic Studies. [in Ukrainian].

Rozumnyi, M.M., Stepyko, M. T., Yablonskyi, V. M. (Eds.). (2012). *Ukrainska politychna natsiia: problemy stanovlennia* [Ukrainian Political Nation: Problems of Formation]. Kyiv, NISS. [in Ukrainian].

Sachkov, Yu. V. (1969). Veroyatnost i razvitie sistemno-strukturnykh issledovaniy [Probability and development of systemic-and-structural research]. In *Systemnye issledovaniia: ezhegodnik* [Systemic research: annual periodical] (pp. 122–139). Moscow: Nauka. [in Russian].

Scott, W. G. (1961). Organizational Theory: An Overview and an Appraisal. *Academy of Management Journal, 4(1),* 7–26.

Secretary-General of the UN. (2013). *Obespetchenie bezopasnosti gosudarstv i obschestv: usilenie kompleksnoi podderzhki, kotoruiu Organizatciia Ob`ediniennyh Natciy okazyvaet reformirovaniiu sektora bezopasnosti* [Securing States and societies: strengthening the United Nations comprehensive support to security sector reform]. Retrieved from https://undocs.org/ru/S/2013/480 [in Russian].

Setrov, M.I. (1988). *Pryntsypy orhanizatsii sotsialnykh system* [Principles of organizing social systems]. Kyiv, Odesa: Vyscha shkola. [in Russian].

Siomin, S.V., & Reznikova, O.O. (2017). Problemy reformuvannia systemy pidhotovky kadriv dlia sektoru bezpeky i oborony Ukrainy [The problems of reforming of the training system for national security and defence sector of Ukraine]. *Stratehichna panorama, 1,* 67–73. [in Ukrainian].

Skaletskyi, Yu.M., Biriukov, D.S., Martiusheva, O.O., & Yatsenko, L.D. (2012). *Problemy vprovadzhennia kultury bezpeky v Ukraini* [Issues of establishing the culture of security in Ukraine]. Kyiv: NISS. Retrieved from http://old2.niss.gov.ua/content/articles/files/kultura_bezp-1bcf6.pdf [in Ukrainian].

Smil, V. (2012). *Globalnye katastrofy i trendy: sleduyschie 50 let* [Global catastrophes and trends: the next 50 years]. Moscow: AST-Press Kniga. [in Russian]

Smolianiuk, V.F. (2018). Systemni zasady natsionalnoi bezpeky Ukrainy [Systemic basic for Ukraine’s national security]. *Visnyk Natsionalnoho universytety “Yuridychna akademiia Ukrainy imeni Yaroslava Mudroho, 2,* 107–126. [in Ukrainian].

Stockholm Resilience Centre. (n.d.). Resilience dictionary. Retrieved from www.stockholmresilience.org/research/resilience-dictionary.html

Sukhodolia, O.M. (2018). Stiykist enerhetychnoi systemy chy stiykist enerhozabezpechennia spozhyvachiv: postanovka problemy [Resilience of energy system or consumers' energy supply: a problem statement]. *Stragehichni priorytety, 2,* 101–117. [in Ukrainian].

Swedish Civil Contingencies Agency. (2019). *Building Resilience in the Nordic Region. A Swedish Perspective.* Retrieved from https://rib.msb.se/filer/pdf/28840.pdf

Sytnyk, H.P., Abramov, V.I., Mandrahelia, V.A., Shevchenko, M. M., & Shypilova, L. M. (2012). Obhruntuvannia kontseptualnykh ta orhanizatsiyno-pravovykh zasad rozrobky pasportiv zahroz natsionalniiy bezpetsi Ukrainy [Justifications for conceptual and legal framework of developing Ukraine's national security threats catalogue]. Kyiv: NADU.

Sytnyk, H.P. (2010). Derzhavna polityka ta osnovy stratehichnoho planuvannia zabezpechennia natsionalnoi bezpeky [Public policy and foundations of strategic planning in support of national security]. In *Kontseptualni zasady zabezpechennia natsionalnoi bezpeky Ukrainy* [Conceptual basis for national security of Ukraine]. Vol. 3. Kyiv: NADU. [in Ukrainian].

Sytnyk, H.P. (2011). Natsionalna bezpeka [National security]. In *Entsyklopedia derzhavnoho upravlinnia* [Encyclopedia of public administration]. Vol. 1. Kyiv: NADU. [in Ukrainian].

Tama, J. (2016). Why Strategic Planning Matters to National Security. *Lawfare*. Retrieved from https://www.lawfareblog.com/why-strategic-planning-matters-national-security

Tarry, S. (2021). *How does NATO support Allies` resilience and preparedness?* Retrieved from https://www.nato.int/cps/en/natohq/news_184730.htm

The Netherlands National Coordinator for Security and Counterterrorism. (2019a). *Countering state threats.* Retrieved from https://english.nctv.nl/themes/state-threats/documents/publications/2019/04/06/countering-state-threats

The Netherlands National Coordinator for Security and Counterterrorism. (2019b). *National Security Strategy 2019.* Retrieved from https://english.nctv.nl/topics/national-security-strategy

The Netherlands National Coordinator for Security and Counterterrorism. (2019c). *National Risk Assessment 2019.* Retrieved from https://english.nctv.nl/documents/publications/2019/09/18/dutch-national-risk-assessment

The Netherlands National Network of Safety and Security Analysts. (2016). *National Risk Profile 2016.* Retrieved from https://www.rivm.nl/sites/default/files/2018-11/Dutch%20National%20Risk%20Profile%202016_english.pdf

The Netherlands National Network of Safety and Security Analysts. (2018). *About The National Network of Safety and Security Analysts*. Retrieved from https://www.rivm.nl/en/about-rivm/organisation/centre-for-environmental-safety-and-security/national-network-of-safety-and-security-analysts

The Netherlands National Network of Safety and Security Analysts. (2019). *Horizonscan Nationale Veiligheid 2019.* Analistennetwerk Nationale Veiligheid. Retrieved from https://www.rivm.nl/sites/default/files/2019-11/Horizonscan%20nationale%20veiligheid%202019.pdf

Thompson, E. P. (1982). *Beyond the cold war*. London: Merlin Press.

UK Cabinet Office. (2011). *Strategic National Framework on Community Resilience.* Retrieved from https://www2.oxfordshire.gov.uk/cms/sites/default/files/folders/documents/fireandpublicsafety/emergency/StrategicNationalFramework.pdf

UK Cabinet Office. (2013). *The role of Local Resilience Forums.* A reference document. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/62277/The_role_of_Local_Resilience_Forums-_A_reference_document_v2_July_2013.pdf

UK Cabinet Office. (2018a). *Preparation and planning for emergencies.* Retrieved from https://www.gov.uk/guidance/preparation-and-planning-for-emergencies-the-capabilities-programme

UK Cabinet Office. (2018b) *Preparation and planning for emergencies.* The Resilience Capabilities Programme. Guidance. Retrieved from https://www.gov.uk/guidance/preparation-and-planning-for-emergencies-the-capabilities-programme#history

UK Cabinet Office. (2019). *Sector resilience plans.* Retrieved from https://www.gov.uk/government/collections/sector-resilience-plans

UK Government. (2010). *A Strong Britain in an Age of Uncertainty.* The National Security Strategy. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf

UK Government. (2013). *Risk assessment: how the risk of emergencies in the UK is assessed.* Guidance. Retrieved from https://www.gov.uk/guidance/risk-assessment-how-the-risk-of-emergencies-in-the-uk-is-assessed

UK Government. (2015). *A Secure and Prosperous United Kingdom.* National Security Strategy and Strategic Defence and Security Review. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/478936/52309_Cm_9161_NSS_SD_Review_PRINT_only.pdf

UK Government. (2016). *Glossary: Resilience. Evidence on Demand*. UK. 2016. DOI: 10.12774/eod_tg.may2016.sturgessandessex2

UK Government. (2017). *National Risk Register (NRR) of Civil Emergencies.* Retrieved from https://www.gov.uk/government/collections/national-risk-register-of-civil-emergencies

UK Government. (2018). *National Security Capability Review.* Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/705347/6.4391_CO_National-Security-Review_web.pdf

UK Ministry of Defence. (2018). *Global Strategic Trends. The Future Starts*

Today. Sixth Edition. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/771309/Global_Strategic_Trends_-_The_Future_Starts_Today.pdf

UK National Cyber Security Center. (n.d.). *Growing positive security cultures.* Retrieved from https://www.ncsc.gov.uk/blog-post/growing-positive-security-cultures

UK Parliament. (2002). *Memorandum from the Civil Contingencies Secretariat.* Retrieved from https://publications.parliament.uk/pa/cm200102/cmselect/cmdfence/518-i/2011602.htm

UK Parliament. (2004). *Civil Contingencies Act.* Retrieved from https://www.legislation.gov.uk/ukpga/2004/36/contents

Ullman, R. (1983). Redefining Security. *International Security, 8(1),* 129–153.

UN-Habitat. (n.d.). *City Resilience Profiling Programme.* Retrieved from https://unhabitat.org/programme/city-resilience-profiling-programme

United Nations Conference on Trade and Development [UNCTAD]. (2020). *The Covid-19 Shock to Developing Countries: Towards a "whatever it takes" programme for the two-thirds of the world's population being left behind.* Retrieved from https://unctad.org/system/files/official-document/gds_tdr2019_covid2_en.pdf

United Nations Development Programme [UNDP]. (n.d.). *UNDP Integrated Project Portfolio. Building Resilience: In response to the Syria Crisis: Regional Refugee & Resilience Plan (3RP) in Response to the Syria Crisis (SRP).* Retrieved from https://www.arabstates.undp.org/content/rbas/en/home/library/CPR/building-resilience--in-response-to-the-syria-crisis-.html

United Nations Development Programme [UNDP]. (1994). *Human Development Report 1994.* Oxford: Oxford University Press. Retrieved from http://hdr.undp.org/sites/default/files/reports/255/hdr_1994_en_complete_nost ats.pdf

United Nations Development Programme [UNDP]. (2008). *A Guide to the Vulnerability Reduction Assessment.* Retrieved from https://www.adaptation-undp.org/resources/training-tools/users-guide-vulnerability-risk-assessment-english

United Nations Educational, Scientific and Cultural Organization [UNESCO]. (2010). *Glossary of basic terminology on disaster risk reduction.* Office Bangkok and Regional Bureau for Education in Asia and the Pacific. Retrieved from https://unesdoc.unesco.org/ark:/48223/pf0000225784

United Nations [UN] General Assembly. (2000). *United Nations Millennium Declaration.* General Assembly Resolution A/RES/55/2. Retrieved from https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A_RES_55_2.pdf

United Nations [UN] General Assembly. (2015). *Transforming Our World: The 2030 Agenda for Sustainable Development.* General Assembly Resolution A/RES/70/1. Retrieved from https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A_RES_70_1_E.pdf

United Nations [UN] General Assembly. (2016). *New Urban Agenda.* Document A/RES/71/256. Retrieved from https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A_RES_71_256.pdf

United Nations International Strategy for Disaster Reduction [UNISDR] (2009). *UNISDR Terminology on disaster risk reduction*. Retrieved from https://www.preventionweb.net/files/7817_UNISDRTerminologyEnglish.pdf

United Nations Office for Disaster Risk Reduction [UNDRR]. (n.d.). *Online glossary*. Retrieved from https://www.undrr.org/terminology

United Nations Office for Disaster Risk Reduction [UNDRR]. (2019). Global Assessment Report on Disaster Risk Reduction. Geneva, Switzerland. Retrieved from https://gar.undrr.org/sites/default/files/reports/2019-

05/full_gar_report.pdf

United Nations Refugee Agency [UNHCR]. (n.d.). *2018–2019 Regional Refugee & Resilience Plan in Response to the Syria Crisis.* Retrieved from https://www.unhcr.org/partners/donors/5a54c1957/2018-2019-regional-refugee-resilience-plan-response-syria-crisis.html

United Nations [UN] Security Council. (2014). *Resolution S/RES/2151(2014).* Retrieved from https://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/2151(2014)

United Nations [UN] Security Council. (2017a). *Resolution S/RES/2341(2017).* Retrieved from https://undocs.org/S/RES/2341(2017)

United Nations [UN] Security Council. (2017b). *Resolution S/RES/2395(2017).* Retrieved from https://undocs.org/S/RES/2395(2017)

United Nations [UN] Security Council. (2017c). *Resolution S/RES/2396(2017).* Retrieved from https://undocs.org/S/RES/2396(2017)

United Nations. (n.d.). *Agenda for Humanity.* Annex to the Report of the Secretary-General for the World Humanitarian Summit. Retrieved from https://sustainabledevelopment.un.org/content/documents/2282agendaforhumanity.pdf

United Nations. (1994). *Yokohama Strategy and Plan of Action for a Safer World. Guidelines for Natural Disaster Prevention, Preparedness and Mitigation.* World Conference on Natural Disaster Reduction. Yokohama, Japan, 23–27 May 1994. Retrieved from https://digitallibrary.un.org/record/161609

United Nations. (2005). *Hyogo Framework for Action 2005–2015: Building the Resilience of Nations and Communities to Disasters.* World Conference on Disaster Reduction. 18–22 January 2005, Kobe, Hyogo, Japan. Retrieved from https://www.unisdr.org/2005/wcdr/intergover/official-doc/L-docs/Hyogo-framework-for-action-english.pdf

United Nations. (2015a). *Sendai Framework for Disaster Risk Reduction 2015–2030.* Adopted at the Third UN World Conference on Disaster Risk Reduction in Sendai, Japan, on March 18, 2015. Retrieved from https://www.undrr.org/publication/sendai-framework-disaster-risk-reduction-2015-2030

United Nations. (2015b). *The Paris Agreement.* Retrieved from https://unfccc.int/sites/default/files/english_paris_agreement.pdf

United Nations. (2017). *United Nations Plan of Action on Disaster Risk. Towards a Risk-informed and Integrated Approach to Sustainable Development.* Reduction for Resilience. Retrieved from https://www.preventionweb.net/files/49076_unplanofaction.pdf

USAID/ENGAGE. (2018). *Hromadkyi aktyvizm ta stavlennia do reform: suspulna dumka v Ukraini (lystopad-hruden 2018)* [Social activism and attitude towards reforms: public opinion in Ukraine (November-December 2018)]. National poll by USAID/ENGAGE on social involvement. Retrieved from https://engage.org.ua/hromadskyj-aktyvizm-ta-stavlennia-do-reform-suspilna-dumka-v-ukraini/ [in Ukrainian].

USAID/ENGAGE. (2021). *Zroby za mene: ukraintsi hotovi do samoorhaniztsii, ale pokladaut vidpovidalnist za sviy dobrobut na derzhavu* [Do for me: Ukrainians are ready for self-organization but hold the government responsible for their well-being]. National poll as to public involvement. Retrieved from https://engage.org.ua/zroby-za-mene-ukraintsi-hotovi-do-samoorhanizatsii-ale-pokladaiut-vidpovidalnist-za-svij-dobrobut-na-derzhavu/

US Department of Homeland Security. (2014). *The 2014 Quadrennial Homeland Security Review.* Retrieved from https://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf

US Homeland Security Council. (2007). *National Strategy for Homeland Security*. Retrieved from https://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf

US National Intelligence Council. (2021). *Global Trends 2040: A More Contested World.* Retrieved from https://www.dni.gov/files/ODNI/documents/assessments/GlobalTrends_2040

.pdf

Uyemov, A.I. (1969). Lohicheskii analiz sistemnoho podkhoda k obiektam i ego mesto sredi druhikh metodov issledovaniia [Logical analysis of a systemic approach to objects and its place amongst other research methods]. In *Systemnye issledovaniia: ezhegodnik* [Systemic research: annual periodical] (pp. 80–96). Moscow: Nauka. [in Russian].

Van Gigch, J. (1981). *Prikladnaya obschaya teoriia system* [Applied General Systems Theory]. Moscow: MIR. Volume 1. [in Russian].

Van Gigch, J. (1981). *Prikladnaya obschaya teoriia system* [Applied General Systems Theory]. Moscow: MIR. Volume 2. [in Russian].

Vinohray, Ye.H. (1989). *Obschaya teoriia organizatsii i sistemno-organizatsionnyi podkhod* [General theory for organization and system-and-organizational approach]. Tomsk: Tomsk university. [in Russian].

Walker, J., & Cooper, M. (2011). Genealogies of resilience: From systems ecology to the political economy of crisis adaptation. *Security Dialogue, 42(2),* 143–160.

Walklate, S., McGarry, R., & Mythen, G. (2013). Searching for Resilience: A Conceptual Excavation. *Armed Forces & Society, 40(3),* 408–427.

Walsh-Dilley, M., & Wolford, W. (2015). (Un)Defining resilience: subjective understandings of "resilience" from the field. *Resilience*, 3(3), 173– 182.

Walters, C. J. (1986). *Adaptive Management of Renewable Resources.* New York: McGraw Hill.

Waters, T. (2015). Politics as a vocation. In T. Waters & D. Waters (Eds.). *Weber's Rationalism and Modern Society*. Palgrave MacMillan. Retrieved from https://www.researchgate.net/publication/305279035_Politics_as_a_Vocation_by_Max_Weber_in_Weber's_Rationalism_and_Modern_Society_edited_and_translated_by_Tony_Waters_and_Dagmar_Waters

Wet veiligheidsregio's [Security Regions Act]. (2010). Retrieved from https://wetten.overheid.nl/BWBR0027466/2019-01-01 [in Dutch].

Williams, P. D., & McDonald, M. (Eds.). (2018). *Security Studies. An Introduction.* 3rd edition. London: Routledge. https://doi.org/10.4324/9781315228358

Wilson, G. (2012). *Community Resilience and Environmental Transitions*. London: Routledge.

World Bank. (2012). *Doklad o mirovom razvitii 2011: konflikty, bezopasnost, razvitie* [World Development Report 2011: conflicts, security, and development]. Moscow: Izdatelstvo "Ves Mir". [in Russian].

World Economic Forum [WEF]. (n.d.). *Global Future Councils Nominations 2020–2021 Terms.* Retrieved from http://www3.weforum.org/docs/WEF_2020_2021_GFC_Concept_Note.pdf

World Economic Forum [WEF]. (2013). Building National Resilience to Global Risks: Special Report. In *The Global Risks 2013: Report, 8th edition*. Retrieved from http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2013.pdf

World Economic Forum [WEF]. (2014). *The Global Risks 2014.* Report, 9th Edition. Retrieved from http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf

World Economic Forum [WEF]. (2015). *Building Resilience in Nepal through Public-Private Partnerships.* Global Agenda Council on Risk & Resilience: Report. Retrieved from http://www3.weforum.org/docs/GAC15_Building_Resilience_in_Nepal_report_1510.pdf

World Economic Forum [WEF]. (2016a). Pathways to Resilience. In *The Global Risks 2016: Report, 11th edition.* Retrieved from http://www3.weforum.org/docs/GRR/WEF_GRR16.pdf

World Economic Forum [WEF]. (2016b). *Resilience Insights.* The Global Agenda Council on Risk & Resilience. Retrieved from http://www3.weforum.org/docs/GRR/WEF_GAC16_Risk_Resilience_Insights.pdf

World Economic Forum [WEF]. (2018). *Cyber Resilience Playbook for Public-Private Collaboration.* Retrieved from http://www3.weforum.org/docs/WEF_Cyber_Resilience_Playbook.pdf

World Economic Forum [WEF]. (2020a). *Building Resilience in Manufacturing and Supply Systems in the COVID-19 context and beyond: Latin America Perspectives.* Regional insight. 2020. Retrieved from http://www3.weforum.org/docs/WEF_Resilience_in_manufacturing_and_supply_systems_LATAM_2020.pdf

World Economic Forum [WEF]. (2020b). *Systems of Cyber Resilience: Secure and Trusted FinTech.* Retrieved from http://www3.weforum.org/docs/WEF_Systems_Cyber_Resilience_2020.pdf

World Economic Forum [WEF]. (2021a). *Principles for Strengthening Global Cooperation.* Retrieved from http://www3.weforum.org/docs/WEF_Global_Action_Group_Principles_2021.pdf

World Economic Forum [WEF]. (2021b). *The Global Risks 2021.* Report, 16th Edition. Retrieved from http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf

World Humanitarian Summit [WHS]. (n.d.) *Grand Bargain.* Retrieved from https://interagencystandingcommittee.org/grand-bargain

Zebrowski, C. The nature of resilience. *Resilience*, *1(3),* 159–173.

Zhalilo, Ya. A., Bazyliuk, Ya.B., Kovalivska, S.V., Kolomiets, O.O., Berezhnyi, Ya. M., Sobkevych, O. V., …Yatsenko, L. M. (2020). *Ukraina pislia koronakryzy – shliakh oduzhannia* [Ukraine following the coronacrisis – the way for recovery]. Kyiv: NISS. Retrieved from https://niss.gov.ua/publikacii/analitichni-dopovidi/ukraina-pislya-koronakrizi-shlyakh-oduzhannya

Annexes

Annex 1
Status of Key Strategic Indicators under the Sustainable Development Strategy “Ukraine - 2020”

Strategic performance indicators of the Strategy	Target value	Actual result	
		2019	2020
World Bank Doing Business Ranking	Top 30	71	64
Global Competitiveness Index of the World Economic Forum (WEF), rank	Top 40	85	n/a
S&P Foreign Currency Credit Rating, category	BBB or higher	B	B
GDP per capita, PPP (according to World Bank), US$	16,000	13,350.5	13,056.7
Foreign direct investment, net inflows in 2015-2020 (according to World Bank), bln US$	> 40	18	18,8
Corruption Perceptions Index of the Transparency International	Top 50	120	122
Life expectancy at birth, years (according to World Bank)	Raise by 3 years	Raised by 1 year over 2015-2019	-
INSEAD Global Talent Competitiveness Index	Top 30	63	66
Level of public trust in law enforcement agencies (according to Razumkov Center), %	70	43...61	37...63
Level of trust of the expert community in court (according to USAID Justice Sector Reform Program “New Justice”), %	70	41*	27
Energy intensity in oil equivalent, per $1000 of GDP (according to the International Energy Agency)	0.2 t	0.25 t*	n/a
The share of local budgets in the consolidated state budget, %	65 or more	21	21
The Ratio of Government Debt to GDP in Ukraine (according to IMF), %	3 or less	2.3	5.2
The total public debt and government-guaranteed loans to GDP (according to IMF), %	60 or less	49	60
Defense and security expenditure, % of GDP	3 or more	5.5	5.9

Note: * - data as of 2018

Source: Compiled by the author based on the information of the State Statistics Service of Ukraine, Ministry of Finance of Ukraine, IMF, WEF, World Bank, International Energy Agency, Razumkov Center, USAID Justice Sector Reform Program "New Justice", INSEAD, Standard and Poors, and Transparency International.

Annex 2
The National Threat and Emergency Response Systems of Ukraine Based on the Interagency Cooperation

Purpose	Organization subsystems/specifics	Major objectives
Unified State Civil Protection System of Ukraine		

To provide the implementation of national policy for civil protection in peacetime, crisis or wartime	Functional and territorial subsystems. *Major actors*: 1) permanent command authorities for civil protection (Cabinet of Ministers of Ukraine, State Emergency Service of Ukraine and its territorial units, authorized central executive authorities, local state administrations, executive committees of local authorities, heads of enterprises, organizations, etc.); 2) coordinating bodies (state, regional, local, and object commissions for technogenic and ecological safety and emergencies); 3) civil protection forces of functional and territorial subsystems	To take measures to: a) ensure the readiness of state and local authorities as well as any of their subordinated means and forces to prevent and respond to emergencies; b) prevent the emergencies; c) support the continuous operation of enterprises, institutions, and organizations as well as reduce the possible material losses. To analyze the information on emergencies; forecast and assess the impacts of emergencies, and determine the need for use of forces, means, and material and financial resources. To teach the population about the proper response to emergencies. To spread the information on the protection of population and territories from the impacts of emergencies; to warn the population on the risk or occurrence of emergencies; to report on the actual situation and measures taken in a timely and accurate manner. To provide for the establishment, rational conservation, and use of material and financial reserves required to prevent or respond to emergencies. To protect the population in case of emergencies, to undertake the rescue and other immediate operations designed to mediate the impacts of emergencies; to ensure the life support services for the affected population, etc.
National counter-terrorism system		
To prevent, respond, and terminate the terrorist acts as well as to mitigate their impacts	Functional and territorial subsystems. *Major actors:* 1) For territorial subsystem – coordination groups of the Anti-Terrorist Center at regional offices of the Security Service of Ukraine and their HQs; 2) For functional subsystem	To prevent terrorist activity through timely identification and elimination of causes and conditions that promote terrorism. To inform the population of the threat level and committed terrorist acts. To secure the possible targets for terrorist attacks.

	– structural units of the counter-terrorism agencies and the Interdepartmental Coordination Commission of the Anti-Terrorist Center at the Security Service of Ukraine.	
National cybersecurity system of Ukraine		
To ensure the cybersecurity, including cryptographic, technical, and other forms of protection for national information resources; to provide cybersecurity for critical information infrastructure as well as to establish cooperation on cybersecurity matters with national and local authorities, military forces, law enforcement agencies, research and educational institutions, public associations, enterprises, institutions and organizations of all form of ownership, operating in the area of electronic communications and information security and/or owners (administrators) of critical information infrastructure	The system is based on the functional principle without any subsystems and clearly defined operating principles for the territorial level. *Major actors*: State Service of Special Communication and Information Protection of Ukraine, National Police of Ukraine, Security Service of Ukraine, Ministry of Defence of Ukraine and the General Staff of the Armed Forces of Ukraine, intelligence agencies, National Bank of Ukraine	To ensure the coordination between cybersecurity agencies and joint protection against cyber threats. To facilitate the establishment and operation of the National Telecommunication Network as well as the implementation of the organizational and technical model for cybersecurity. To prevent, identify and respond to cyber incidents and cyber-attacks as well as to eliminate their impacts. To inform on the cyber threats and protection mechanisms. To ensure the protection of rights and freedoms of people as well as the interests of society and the state from criminal attacks in cyberspace. To take measures designed to prevent, detect, suppress and investigate cybercrimes. To spread the security-related knowledge in cyberspace. To counter cyber terrorism and cyber intelligence. To facilitate the readiness of the critical infrastructure for possible cyber-attacks and cyber incidents, etc.
Defense capability ensuring system of Ukraine		
To ensure the readiness and capability of all actors of the	The system is based on the functional principle. The organizational features of the Territorial Defense have been	To prepare for defense, including: - To project and assess the military threat and the war danger; - To develop and implement the

security and defense sector of Ukraine, national and local authorities, the unified state system of civil protection of Ukraine as well as national economy for the transition from a state of peace to a state of war; defense against armed aggression, and termination of an armed conflict as well as the readiness of the population and national territory for defense	identified. *Major actors:* 1) in the field of defense capacity and coordination of respective activity within Ukraine: National Security and Defense Council of Ukraine, the Cabinet of Ministers of Ukraine, the Ministry of Defence of Ukraine, and the General Staff of the Armed Forces of Ukraine; 2) in the field of defense capacity, at the territorial level: local administrations, local self-government authorities, including executive committees, and military commissariats	military, military-economic, military-technical, and national military-industrial policy; - To improve the structure, specify the tasks, and functions of the Armed Forces of Ukraine and other uniformed services; to ensure the required strength of the personnel, development, training, and appropriate level of combat capability, as well as combat and mobilization readiness for national defense; draft the employment planning; - To develop the military-industrial complex, establish favorable conditions for mobilization of various national industries designed for the production of a sufficient number of weapons, materiel and military equipment; - To plan and prepare the resistance movement; - To ensure the readiness of national and local authorities and the unified state system of civil protection for operation in a wartime; - To establish the state material reserves and reserve funds; - To protect the national borders of Ukraine; - To ensure the cyber defense measures for the protection of national sovereignty and defense capability, to prevent an armed conflict, and to counter armed aggression; - To develop the territorial defense; - To defend against armed aggression etc. Objectives of territorial defense: - To protect and secure the state border; - To facilitate the continuous operation of public authorities, military command and control bodies, as well as strategic (operational) deployment of forces; - To protect the important facilities and communications; - To eliminate the sabotage-reconnaissance forces, other armed formations of the aggressor, and illegal

		armed groups acting against the state; - To maintain the legal regime of martial law.
Emergency medical services system		
To ensure the organization and performance of life-saving measures for people in urgent state and reduce its impact on health, including in case of emergencies and response to them.	The system is based on the functional principle. The special features of the organization and the supply of its operations on a territorial level have been identified. *Major actors*: health care institutions and their structural units (emergency and disaster medicine centers, emergency (ambulance) stations, emergency (ambulance) crews, emergency (rescue) departments responsible for the organization and provision of emergency medical assistance.	To provide accessible, free, timely, and quality emergency health care, including in case of emergencies and response to them. To provide medical and sanitary support during mass events and activities involving state-protected individuals. To maintain cooperation with emergency rescue units of the ministries as well as central and local executive authorizes during emergencies and response to them.

Source: Reznikova et al. (2021) (amended by the author).

Annex 3
Self-Assessment Survey for Executive Authorities on Resilience

(name of institution)

I. Security situation analysis

1. Which are the core indicators for the state of security of the industry (areas of responsibility)?

2. Do those indicators exceed or approach the critical level?

□ YES □ NO

(If NO, go to Q 4 of the survey)

3. If the indicators exceeded the critical values, what caused this situation?

4. Is the current situation in the industry (area of responsibility) getting any worse?

□ YES □ NO

5. Which factors may be detrimental to the current situation?

6. Which is the largest threat to the industry (area of responsibility)?

(In case of more than one threat, apply Q7-11 to each threat)

7. Which target groups/objects are the most vulnerable to current threat impact?

8. What could be the most extensive negative impact of the threat on the target group provided in Q7? *(Provide an answer for every target group)*

9. Which factors hurt the ability of the most vulnerable target groups/objects to resist the threat?

10. Which target groups/objects are capable of dealing with the threat on their own at acceptable losses in functionality?

11. Are the indicators and limits of permissible losses in the industry (area of responsibility) defined in terms of target groups/objects?

□ **YES** □ **NO**

II. Capability analysis
(The answers to these questions should be provided by separate public entities and enterprises, which are subordinated to the ministry (agency). The answers to Q1-11 should be provided for each identified threat separately).

Indicate the type of threat

1. Assess the sufficiency of core resources to counter the identified threat and mark your answer for every type of resource in the appropriate cell of the table.

	meets predetermined standards	*insufficient*	*critically insufficient*
human			
material			
financial			

2. Are there any unregulated legal matters within the industry (area of responsibility) that complicate the response to an identified threat?

□ **YES** □ **NO**

If YES, indicate them.

3. Are there any unresolved administrative matters within the industry (area of responsibility) that complicate the response to an identified threat?

□ **YES** □ **NO**

If YES, indicate them.

4. Have there been exercises, training sessions on different stages of response to the identified threat or development of the relevant crises?

□ **YES** □ **NO**

5. Do all entities that respond to an identified threat clearly understand the course of joint actions and their area of responsibility?

□ **YES** □ **NO**

6. Identify the most challenging issues of interdepartmental cooperation in countering the identified threat.

7. Is the population well informed of the possible signals of threat or crisis?

□ **YES** □ **NO**

8. Is the population well informed of the procedure for dealing with a threat or crisis?

□ YES	□ NO

9. Is there an established two-way channel of communication between the ministry (agency) and the population on crisis response matters?

□ YES	□ NO

10. Is there an established two-way channel of communication on matters of cooperation and crisis response between the ministry (agency) and

Other authorized public authorities	□ YES	□ NO
Subordinate institutions, enterprises, and organizations	□ YES	□ NO

(Mark your answer in the appropriate cell of the table)

11. Are the necessary (standard) reserves of core resources accumulated?

human	□ YES	□ NO
material	□ YES	□ NO
financial	□ YES	□ NO

(Mark your answer in the appropriate cell of the table)

12. Indicate the time required to engage the additional (reserve) resources.

____

____

____

____

____

13. Are there any reserve premises that could be used for the temporary relocation of public institutions and strategic enterprises in case of unavailability of main premises?

□ YES	□ NO

14. Is there any alternative energy supply source for the electrical equipment of public institutions or enterprises in case of main supply sources failure?

□ YES	□ NO

15. Is there a minimum necessary reserve (in case of crises) of the following:

personal protection equipment	□ YES	□ NO
potable water	□ YES	□ NO
food products	□ YES	□ NO

(Mark your answer in the appropriate cell of the table)

16. Is there any alternative transport and logistics capacities for the personnel of the public institutions or enterprises in case of the main capacities fail?

□ YES	□ NO

17. Indicate the time required to engage the additional (reserve) capacities of the public institution (enterprise).

18. Is there a chance (in case of crisis) to provide the population with alternative sources of:

potable water	□ YES	□ NO
food products	□ YES	□ NO
electricity	□ YES	□ NO

(Mark your answer in the appropriate cell of the table)

19. Is there any premises allocated for accommodating:

IDPs	□ YES	□ NO
medical facilities	□ YES	□ NO
people affected by the crisis	□ YES	□ NO

(Mark your answer in the appropriate cell of the table)

20. Are the available communication systems capable of providing the reliable and secure transmission of important data?

□ YES	□ NO

21. Do the current cybersecurity systems provide a reliable level of protection?

□ YES	□ NO

22. Is the personnel of the public institution or enterprise provided with equipment for remote operations, including:

mobile technical equipment to work with information	□ YES	□ NO
civilian communication equipment	□ YES	□ NO
protected communication equipment	□ YES	□ NO
other technical equipment (specify which ones):	□ YES	□ NO

(Mark your answer in the appropriate cell of the table)

23. Are there any conditions established for the work of public institution personnel with classified information in remote or other informal mode?

□ YES	□ NO

24. Is there an emergency evacuation procedure for:

population	□ YES	□ NO
strategic enterprises	□ YES	□ NO
public institutions	□ YES	□ NO

(Mark your answer in the appropriate cell of the table)

25. Are there any protocols for a coordinated response to crises?

□ YES	□ NO

26. Are there any scenarios describing the possible development of the crisis?

optimistic	□ YES	□ NO
pessimistic	□ YES	□ NO
optimum	□ YES	□ NO

(Mark your answer in the appropriate cell of the table)

27. Are there any alternative strategies covering the response to the crises?

□ YES	□ NO

Source: developed by the author

Scientific publication

Olga REZNIKOVA

NATIONAL RESILIENCE IN CHANGING SECURITY ENVIRONMENT

Monograph

Design by Pavlo Reznikov

The monograph was prepared for publication
at the National Institute for Strategic Studies
Pyrohova str., 7-a, Kyiv, 01030
Tel./fax: (044) 234-50-07
e-mail: info-niss@niss.gov.ua http://www.niss.gov.ua