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*.

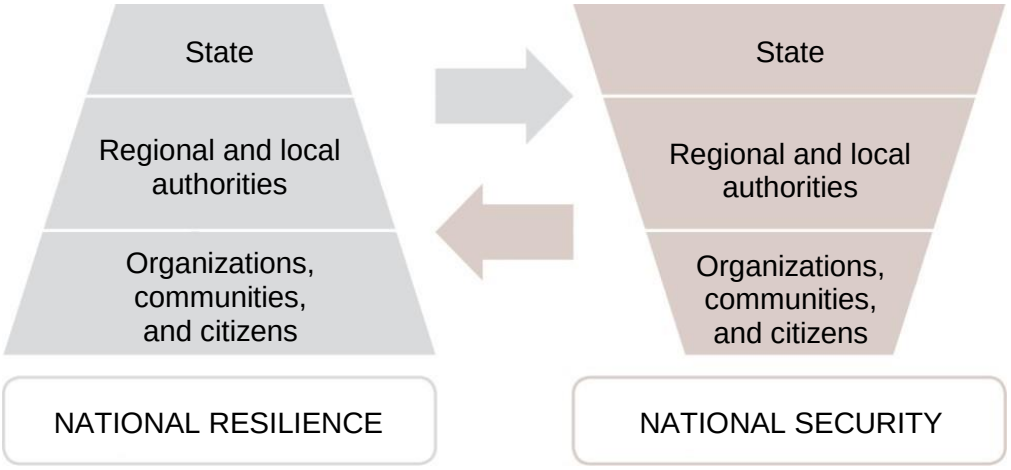

Fig. 2.1. Balancing centralization and decentralization governance principles in a comprehensive system of ensuring national security and resilience
Source: developed by the author.

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.

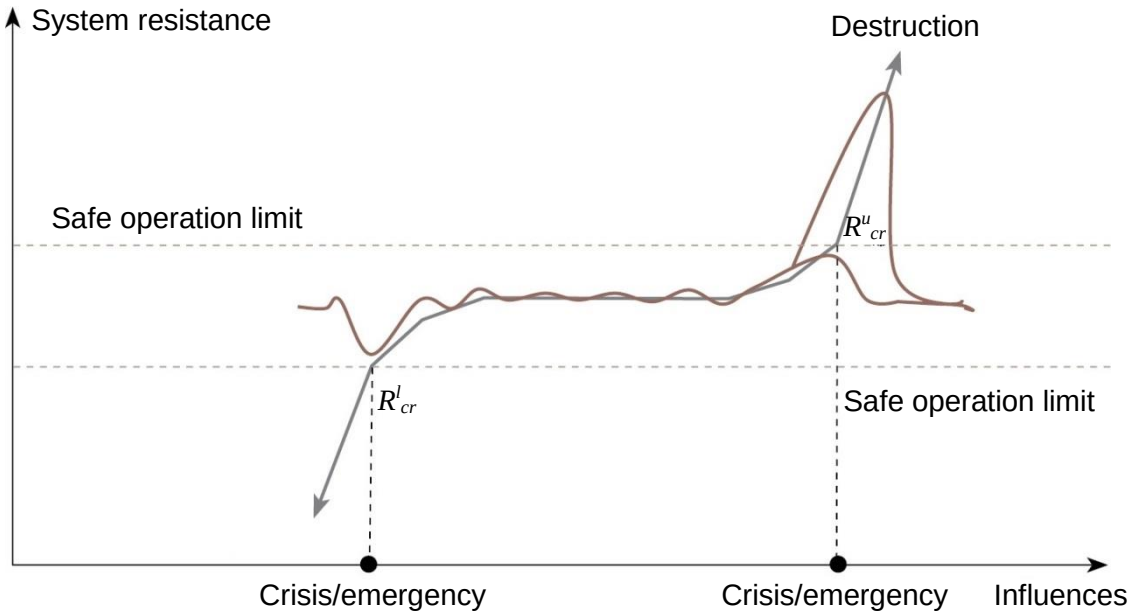

Fig. 2.2. Managing national resilience on the basis of the homeostatic plateau
Source: Van Gigch (1981b), Kharazishvili (2019) (adjusted by developed by the author).

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*.

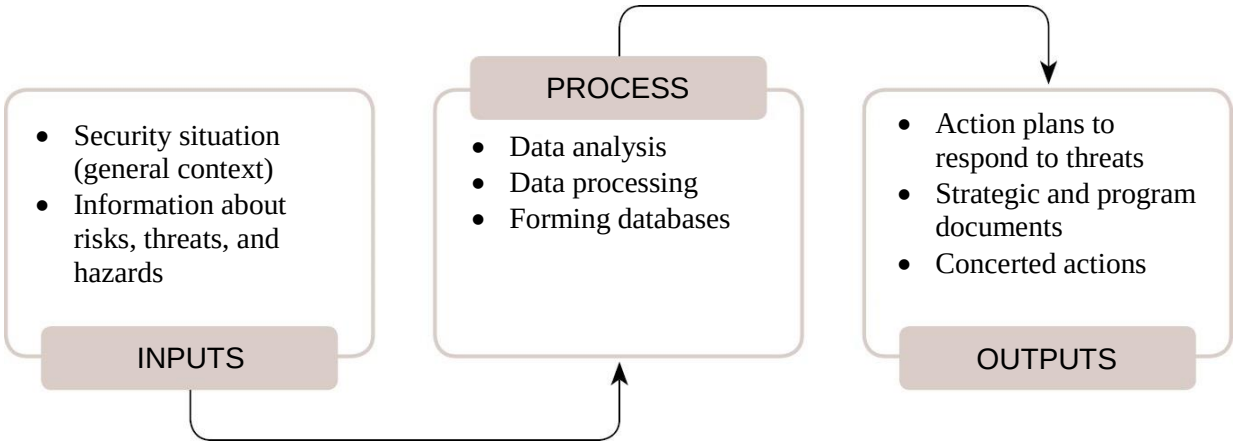

Fig. 2.3. A general scheme of the national risk assessment system operation
Source: developed by the author.

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).

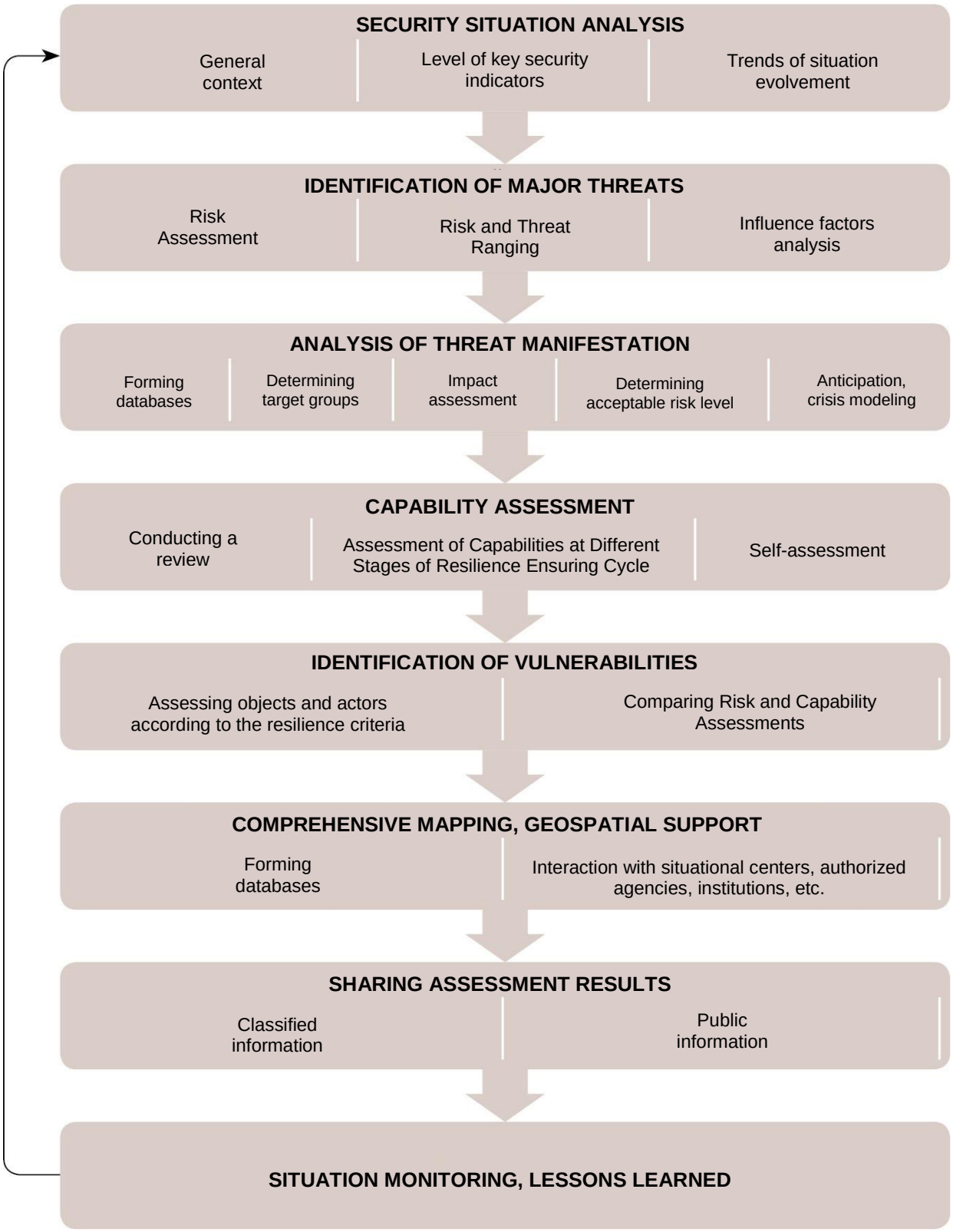

Fig. 2.4. Algorithm for Comprehensive Risk and Capabilities Assessment and Threats and Vulnerabilities Identification

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.*

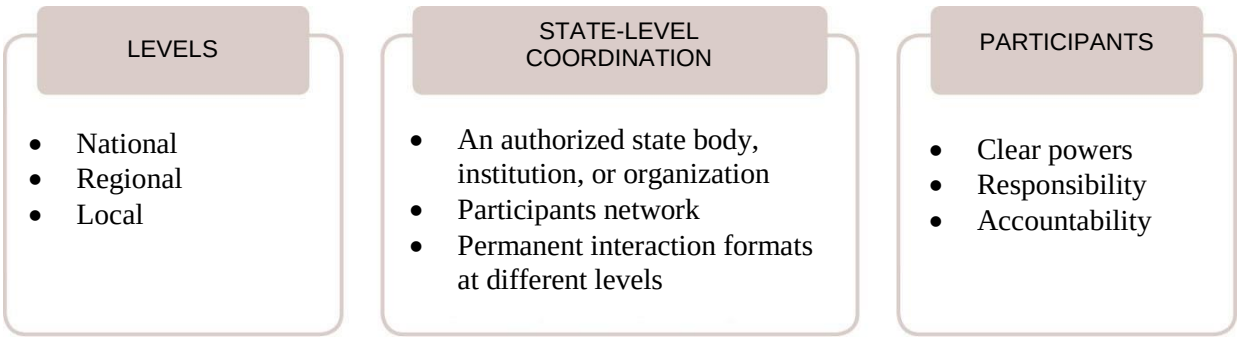

Fig. 2.5. Peculiarities of National Risk Assessment System Organization

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.

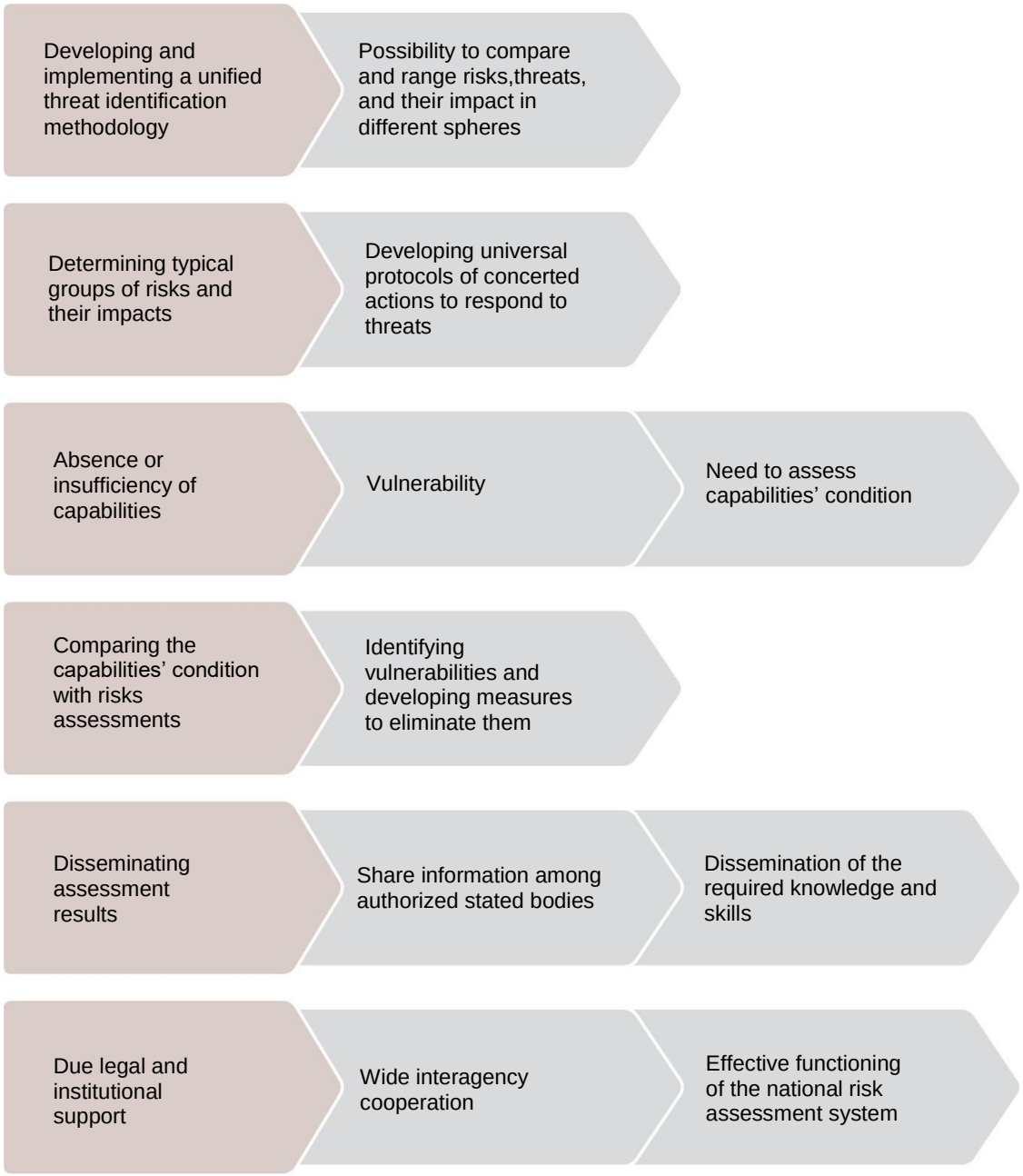

Fig 2.6. Aspects of Essential Importance in Organization and Functioning of National Risk Assessment System

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.

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.

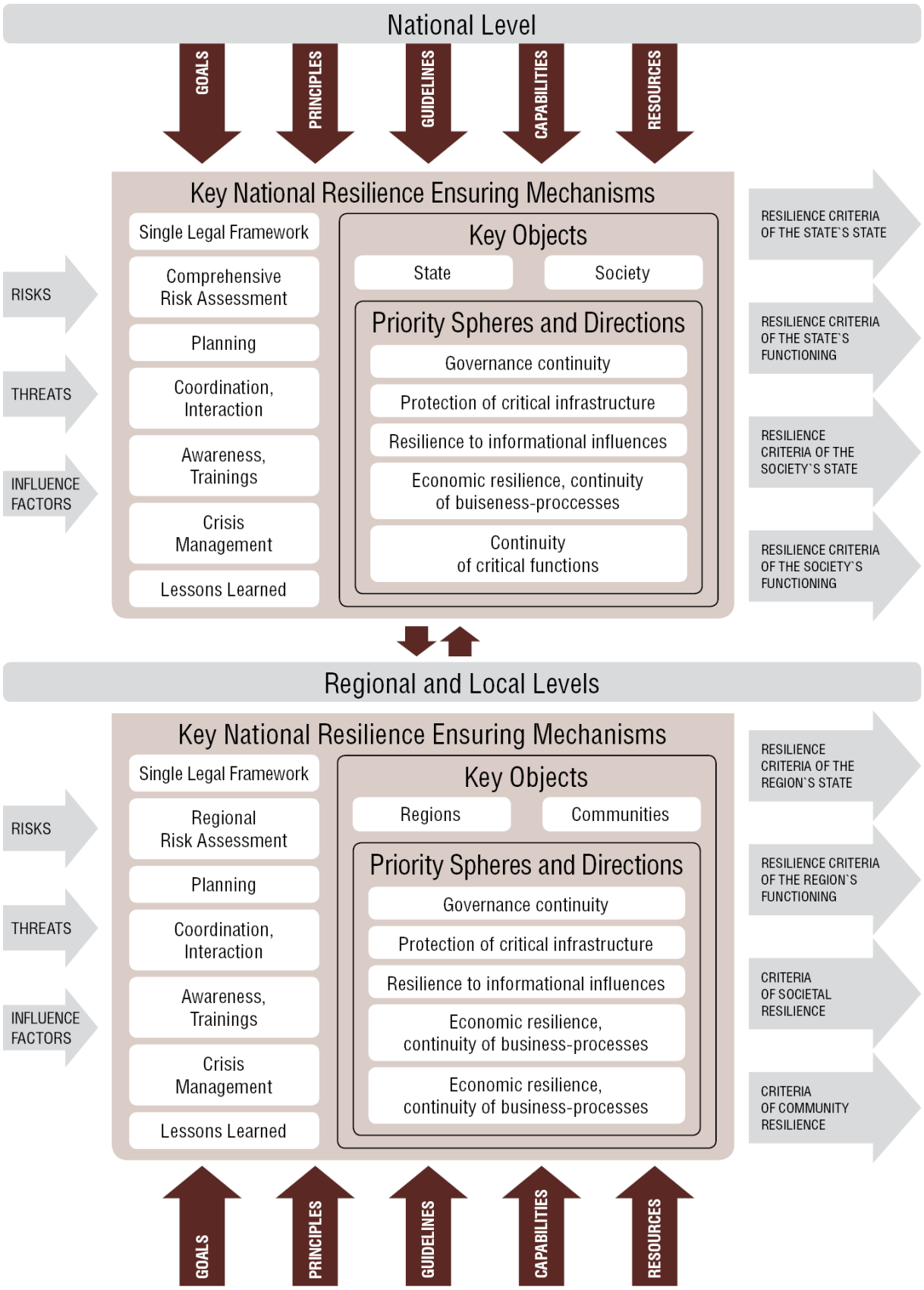

Fig. 2.8. Multi-level comprehensive model of ensuring national resilience

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.