SECTION 3. ECONOMY AND MANAGEMENT OF STATE GRATITUDE

DOI: 10.46299/ISG.2023.MONO.ECON.3.3.1

3.1 Organizational and management ensuring the critical infrastructure development on the basis of public-private partnership

In recent decades, the global world has realized the direct dependence of the sustainable development of national economies and economic growth on safe and stable critical infrastructure [31-42]. At the same time, sustainable functioning and protection of critically important infrastructure facilities can be achieved under the conditions of creating proper institutional, organizational, managerial, financial, and information support on the basis of integrated interaction and effective public-private partnership.

According to a survey conducted in 2020 by The Global Infrastructure Investor Association (GIIA) together with the international research company Ipsos Group, attracting investment in infrastructure development in the context of economic recovery and modernization is recognized as a strategic task in the plans of governments of various countries around the world. At the same time, 79% of respondents note that investments in infrastructure make it possible to create new jobs and increase the level of economic development. And 68% of respondents emphasize the need to prioritize investments in infrastructure as part of the recovery of the national economy. However, 59% claim that the government of their country implements insufficient measures to provide infrastructure for the development of the economy.

It should be noted that various definitions of the concept of “critical infrastructure objects” are used in the countries of the world [43]. Let's consider some of them:

1) Critical infrastructures are those infrastructures, or parts thereof, that are critical to the provision of important social functions. Their failure or destruction has a serious impact on the health, safety or economic and social well-being of the population or the functioning of government institutions (Austrian Cybersecurity Strategy, 2013).

2) Critical infrastructure refers to the processes, systems, facilities, technologies, networks, assets and services necessary for the health, safety, security or economic well-being of Canadians and the effective functioning of government (Emergency Canada, 2011).

3) Vital infrastructure is any institution, facility or structure for which damage, inaccessibility or destruction as a result of a malicious act, sabotage or terrorist act can directly or indirectly: if its activities are difficult to replace or compatible, seriously aggravate military or economic potential, national security or the survival of the nation, or seriously affect the health or life of the population (General Inter-Ministerial Instruction for Life Safety, General Secretariat for Defense and National Security of France).

4) Critical infrastructure are organizational and physical structures and objects of such vital importance to the society and economy of the country, when their failure or degradation leads to persistent supply shortages, significant violations of public safety and security or other dramatic consequences (National strategy for the protection of critical infrastructure facilities, Germany, 2009).

5) System, resource, process, structure, even virtual, destruction, interruption or even partial or temporary unavailability of which leads to a significant weakening of the efficiency and normal functioning of the country, as well as the security and economic, financial and social systems, including central and local public administration (Italian Civil Protection Agency).

6) Critical infrastructure is the building and systems necessary to maintain functions that cover the basic needs of society and the sense of security of the population (Cybersecurity Strategy for Norway).

7) Critical Infrastructure includes the infrastructure designated by any Government of Pakistan and such other assets, systems and networks, whether physical or virtual, so vital to the State or its organs, including the judiciary, that their incapacity or destruction may have a devastating effect on national security, economy, health, security or related issues (Cybercrime Bill, Pakistan, 2015).

8) Physical assets, systems or installations that, if destroyed, compromised or destroyed, could have a serious impact on the health, safety, security or economic well-being of Qatar or on the effective functioning of the Government of Qatar (Qatar Cybersecurity Strategy, 2014).

9) Critical Infrastructure is defined as a system and assets, whether physical or virtual, that are so vital to Saudi Arabia that the failure or destruction of such systems and assets could have a devastating effect on security, national economic security, national health or safety, or any combination of them (Development of a National Information Security Strategy for the Kingdom of Saudi Arabia – NISS Project 7).

10) Critical infrastructures are strategic infrastructures (facilities, networks, systems, and physical and IT equipment that support the operation of essential services that are required) and where alternative solutions are not possible, such that their disruption or destruction could seriously affect essential services (Law of Spain 8/2011).

11) Critical infrastructure refers to infrastructure whose destruction, failure or disruption would have serious consequences for society, the private sector and the state (National Cyber Risk Strategy of Switzerland, 2012).

12) Systems and assets, both physical and virtual, so vital to the United States that the failure or destruction of such systems and assets would have a devastating effect on security, national economic security, national health or safety, or any combination thereof (Anti-U.S. with terrorism in the USA, 2001).

In most countries of the world, the majority of assets of critical infrastructure facilities (CIFs) are privately owned. In addition, private operators are at the forefront of investment and major efforts to develop new production and protection technologies. These circumstances, combined with the fact that the primary responsibility for protecting critical infrastructure assets/systems lies with their owners/operators, emphasize the importance of ensuring effective public-private partnerships (PPPs) to achieve adequate levels of resilience.

When developing strategies for the protection of critical infrastructure, it is necessary to create conditions for effective implementation by: evaluating success factors and disincentives; definition of areas of application and possible forms; anticipating key threats, barriers, constraints and challenges.

The Meridian Process, an open forum for the exchange of ideas on critical infrastructure protection and cooperation between senior government policymakers, identified the following factors that underlie effective public-private partnerships: trust, value, respect, and code of conduct, awareness of opportunities and limitations, realistic expectations.

Public-private partnerships should not focus on one specific stage of the critical infrastructure protection cycle. However, they should cover all stages, from the development and implementation of measures to the stages of risk and crisis management.

The benefits of pooling resources, mutual support and joint decision-making between the public sector and private operators of critical infrastructure facilities extend to areas such as safety assessment; review of security measures [44-45]; identification of critical assets and processes; development of action plans in emergency situations; incident response training, etc.

The most appropriate form of this partnership depends on many factors, such as the objectives, the number of stakeholders to be involved, and whether the partnership is expected to address strategic or operational issues. Public-private partnerships can take many forms, from very informal forms of cooperation to more formal arrangements. The degree of formality is often related to the level of control that state bodies seek to exercise. On the other hand, it has been established that project-oriented public-private partnerships are usually more effective than process-oriented ones. This is due to the fact that project-oriented public-private partnerships usually include clearly defined missions, deadlines and budgets.

Public-private partnerships that are not well-thought-out risk becoming "empty boxes" with little or no added value for the protection of critical infrastructure. To ensure that public-private cooperation arrangements continue to be relevant and

productive efforts, EU countries need to be mindful of the most common causes of failure.

Disadvantages may be related to a gap in expectations between the private and public sectors, unstable funding models, unclear division of labour, etc. A sense of urgency helps create a connection between the public and private sectors, fostering a willingness to collaborate and achieve a common vision. This ultimately allows the partnership to grow. The longevity of the partnership depends on the interaction of these factors and is a dynamic process with periods of both weak and strong indicators. Other problems may be related to the lack of business motivation to invest financial resources to protect their own critical infrastructure facilities.

The Organization for Security and Co-operation in Europe (OSCE) has developed a basic 8-step guide on how countries should maximize the benefits that can be derived from public-private partnerships, leveraging the common interests of all stakeholders.

Although the guidelines have been developed as part of best practice for critical energy infrastructure, they are considered universal and can generally be applied across all sectors:

1) analysis and determination of the motivation of each partner to be included in the critical infrastructure protection partnership to clarify mutual expectations and contributions;

2) determination of the ambitions and goals of the partnership for the protection of critical infrastructure on the basis of common national goals for the protection of important objects;

3) review of the existing regulatory framework, which applies to each critical infrastructure sector; determination of mandatory norms, rules and principles; assessment of the adequacy of the existing regulatory framework, taking into account the expected risks and levels of readiness;

4) provision of protection mechanisms and legal certainty for the exchange of information related to the protection of critical infrastructure objects between all interested parties; providing mechanisms for voluntary efforts, including the

development and sharing of best practices, consultation and dialogue for ongoing and effective partnerships;

5) formation of an institutional structure that promotes inter-organizational cooperation and information exchange; clarifying the role and contribution of each partner (for example, government agencies, owners and operators of critical infrastructure, product suppliers, associations); establishment of guiding principles of cooperation;

6) focusing on one or two critical infrastructure sectors;

7) determination of critical milestones for consideration of what has been achieved and what needs to be done in the future;

8) ensuring an ongoing review process to review and update partnerships to ensure progress is commensurate with the overall risk picture and security measures required for an optimal level of protection.

It is worth noting that in Finland considerable attention is paid to public-private partnerships to ensure the sustainability of critical infrastructure. The National Agency for Emergency Situations (NESA), established in 1993, is responsible for planning, developing and maintaining the security of supplies to Finland. While its historic role of maintaining reserve stocks to protect the livelihoods of the population and the functioning of the economy remains part of its strategic objectives, NESA is increasingly involved in ensuring the continuity and sustainability of business in various sectors of the economy through public-private partnerships.

NESA has established a network of thematic clusters where key critical sector stakeholders develop partnerships for vulnerability and performance assessment and resilience planning. NESA also offers special tools such as information systems, storage and vehicles to ensure business continuity in these areas.

NESA funds specific activities related to business continuity and critical infrastructure protection. The agency prepares annual reports that evaluate the performance of companies in critical sectors, including ratings and specific recommendations.

Among its results, NESA boasts increased public-private partnerships with companies in critical sectors (currently numbering over 1000), which has resulted in the development of a business continuity plan appropriate to their activities and sectors.

Studying the experience of Germany, one can also note active actions on the implementation of public-private partnership tools. Organized in 2007 and adjusted in 2013, UP KRITIS is Germany's public-private critical infrastructure protection platform for sectoral and cross-sectoral cooperation. Mutual trust is at the heart of his work. Participants share know-how and experience and learn from each other regarding the protection of critical infrastructure. Under UP KRITIS, concepts are being developed, contacts are being made, exercises are being conducted, and a collaborative approach to IT crisis management is being created and launched.

At the same time, UP KRITIS is addressing issues that go beyond the field of information technology, based on the recognition that a separate study of physical security and IT security [46, 47, 48] is not enough to achieve the overall goal of protecting critical infrastructure.

Within the framework of UP KRITIS, there are two forms of cooperation: operational-technical cooperation (between all participants) and strategic-conceptual cooperation (in established bodies). It is important to note that business is gradually involved and can become more or less intensive depending on the willingness of companies to actively participate; the goal is to keep the system manageable while reaching out to as many companies as possible from all CI sectors.

In particular, the organization is first integrated into UP KRITIS as a “participant”. All German critical infrastructure operators, national professional and industry associations from the CI sectors, as well as competent government authorities can apply to participate in UP KRITIS. Participants appoint representatives of their organization who are granted access to UP KRITIS products, including confidential information. If an organization wishes to cooperate more actively, it can become a “partner” and apply for the integration of its representatives into sectoral working groups and thematic working groups. Each working group represents its own information network where information can be exchanged on a confidential basis.

Other key components of the organizational structure are the Plenum and the Council. The Plenum is the system's cooperation committee. It operates in all sectors, setting the key strategic directions for UP KRITIS, deciding whether to create or dissolve working groups, planning future joint actions, etc. The Plenum consists of representatives of CI operators, their professional and industry associations, as well as representatives of the public sector. The Council strengthens partnerships and collaborations within UP KRITIS and gives impetus to achieve strategic goals and projects. It also ensures that the platform can perform its tasks with adequate resources and the necessary support from the public and private sectors. The Council is made up of senior politicians from CI operators and the public sector.

Therefore, issues of public-private partnership in the EU countries are being updated and are gaining special importance. At the same time, it is worth emphasizing that in the development of national strategies in European countries, in order to ensure the stability and stability of critical infrastructure, it is necessary to create appropriate conditions by: evaluating the stimulating and destimulating factors; definition of areas of application and possible forms; anticipating key threats, barriers, constraints and challenges.

In further studies, it is planned to substantiate the conceptual principles of critical infrastructure protection from the standpoint of national security of Ukraine, taking into account advanced European practice.