Center for Security Studies

The State Critical Infrastructure Protection System in the National Security System

The Analytical Report

Kyiv 2020

УДК
К64

An electronic version was available on NISS' site - https://niss.gov.ua

Authors

Sergiy I. Kondratov — *Senior researcher at the Department of Critical Infrastructure, Energy Security and Ecological Safety at the National Institute for Strategic Studies, NISS*

Oleksandr M. Sukhodolya — *Head of the the Department of Critical Infrastructure, Energy Security and Ecological Safety at the National Institute for Strategic Studies, NISS*

К64 *Kondratov S.I., Sukhodolia O.M. The State Critical Infrastructure Protection System in the National Security System: the analytical report General edior: Sukhodolia O.M., D.Sc. Professor Kyiv, NISS, 2020. 28 p.*

Organizational and legal issues of ensuring critical infrastructure protection (security) and resilience in terms of management approaches are considered. Basing on the outcome of national experience of a number of countries a direct correlation between critical infrastructure protection (security) and national security is illustrated. As well as a conclusion is made regarding influence of the maturity of the public governance in the field of national security on making choice among organizational and legal approaches to protect vitally important for national infrastructures. Bearing in mind the above mentioned introducing the critical infrastructure protection concept in Ukraine is analyzed. The possible options for development of Ukraine's policy to ensure critical infrastructure protection (security) and resilience are outlined. A number of conclusions and recommendations are made for further steps to achieve progress in this field.

The report is intended for the representatives of public authorities, academia and think tanks, independent experts and all of those who are interested in the topic of critical infrastructure protection (security) and resilience, as well as in issues related with Ukraine's national security.

УДК

CONTENTS

Introduction

It is well known that a leadership role in implementation of the critical infrastructure (CI) concept has played by the U.S. This country was the first where the term *critical infrastructure* was defined. It was happened in 1996. Since then the term definition was clarified several times gaining its current formulation soon after the events of 11 September 2001, namely 26 October 2001, when the USA PATRIOT Act[1] was signed into law by U.S. President George W. Bush. This definition clearly points at direct interconnection between CI conditions and national (homeland) security[2].

The declared in the PATRIOT Act interconnection has been arranged and implemented in various ways including approval of a number legislations as well as in relevant changes in governmental agencies structures, redistribution of their responsibilities, powers, and functions, broader involvement of private companies on a partnership basis,

The United States maintains leadership in this field due to it's continued commitment to application of sound management practices tested in other fields, improvement of information and analytical support to a decision making process, cutting edge technologies implementation, active expanding various forms and formats of training and education regarding different aspects of CI protection (security) and resilience.

Besides, it is worth to note that the U. S. has gained firm awareness of necessity to ensure security and resilience not only national infrastructures but also their supplying chains responsible for providing critical materials, resources, technologies and services thereby expanding best practices application to other activities aiming at national security and national resilience improvement[3].

Other developed countries use widely the approaches developed and tested in the U.S., of course, bearing in mind their national features. Below, the examples of interconnection between national (*state, homeland*) security and CI protection (security) and resilience are presented for several developed countries.

CI protection (security) and resilience issues are on the agenda of a number of international organizations among which for the purpose of this study the most interesting are NATO and EU to membership of which Ukraine is aspiring, as well as

---

[1] The USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001.

URL: https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf .

[2] In the *critical infrastructure* definition the term *homeland security* is used which defines one of the most important components of the *national security.*

[3] See, for example: Executive Order on Delegating Authority Under the DPA with Respect to Food Supply Chain Resources During the National Emergency Caused by the Outbreak of COVID-19.

URL: https://www.whitehouse.gov/presidential-actions/executive-order-delegating-authority-dpa-respect-food-supply-chain-resources-national-emergency-caused-outbreak-covid-19 .

OECD[4], comprising of developed countries adherent to ideas of market economy and representative democracy.

It is worth to note that recent years there has been a global tendency towards broader context of measures aiming at ensuring CI functioning: CI ***protection (security)*** has been considered along with CI ***resilience***. When doing so, national governments have increasingly focused on CI resilience rather than its protection (security). Such a shift of emphasis in the subject matter is due to the emergence of new threats and hazards against rapid evolution and transformation already existing ones. Also, various combinations of threats and hazards are taken into account.

Under such circumstances, no protection (security) system is capable to fully guarantee protection (security) against all threats and hazards. Since whilst a security system is being built up to protect against certain threats and hazards, new ones emerge and develop.

That is why nowadays attention is increasingly paid to ***CI resilience*** — *the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions; includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents (as defined in the U.S. regulations)*[5].

The report focuses on clarifying the potential role and the place of a would-be Statecritical infrastructure protection (security) and resilience system in Ukraine within national security sector basing on other countries experience. In so doing the authors had the aim to convey the idea of inseparability of CI security and resilience and national security to the political leadership in Ukraine rather than to comprehensively describe all multidimensional and multilevel links between the mentioned system and national security issues. A greater awareness of these relationships will promote a coherent and harmonized approach to reforming the national security sector.

Chapter 1 presents an overview of forms the links between CI protection (security) and resilience taken in three developed countries – U.S., Germany and Poland.

Chapter 2 is devoted to a brief overview of ensuring protection (security) of the infrastructure objects and systems usually assigned to CI in GUAM member-states – Georgia, Moldova, and Azerbaijan whose economies are in transition.

Chapter 3 concerns the CI protection (security) concept in terms of maturity of national security and defense governance mechanisms.

In Chapter 4 the issues of the CI and its protection concept implementation in Ukraine are analyzed.

Chapter 5 includes a number of conclusions and recommendations.

[4] The Organization for Economic Cooperation and Development

[5] https://www.dhs.gov/sites/default/files/publications/National%20CISR%20R%26D%20Plan_Nov%202015.pdf

1. The review of legal and regulatory frameworks as well as organizational and management forms in which CI protection (security) and national security links are manifested in the U. S., Germany and Poland

In order to illustrate the main approaches to implementing CI protection concept in its connection with the national security and so doing not to overload the text our attention will be paid to national practices of only three countries assigned to the developed ones, namely the U. S., Germany and Poland.

The links between CI protection (security) conditions and national (*state*, *homeland*) security[6] will be demonstrated through definitions of key terms and some provisions of the legislative and regulatory acts as well as structural links among relevant actors in national security sectors.

1.1. The example of the U. S.

According to the U. S. legislation (*USA PATRIOT Act),* the term

> ***"[C]ritical infrastructure" means systems and assets, whether physical or virtual, so vital to the United States that incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.***

In the first Strategy for Homeland Security (2002), approved to mobilize and organize the nation *to secure the U.S. homeland from terrorist attacks*[7] CI protection was assigned to six critical mission areas of the relevant activities. They are the following:

- Intelligence and Warning;
- Border and Transportation Security;
- Domestic Counterrorism;
- Protecting Critical Infrastructures and Key Assets;
- Defending against Catastrophic Threats;
- Emergency Preparedness and Response.

The homeland security objectives addressing CI protection are implemented through execution of the *National Infrastructure Protection Plans* (NIPPs) which are updated depending on changes in the security landscape.

---

[6] Depending on national specificities and contexts, the terms *national security, homeland security,* and *state security* are either strictly interconnected or, in some cases, even synonimical. For example, in the U.S. *National strategy for homeland security* (2002) (see note 7 below) national security and homeland security were considered as *twin concepts* while the National Security Strategy of the United States and National Strategy for Homeland Security — as *mutually supporting documents*.

[7] National strategy for homeland security/
URL: https://www.dhs.gov/sites/default/files/publications/nat-strat-hls-2002.pdf .

The direct links between national (homeland) security and CI protection (security) are apparently reflected in the U.S. governmental authorities' structures as well. It was especially evident at the early stages of building the national CI protection system in the U.S. which may be interesting for Ukraine (Fig. 1).

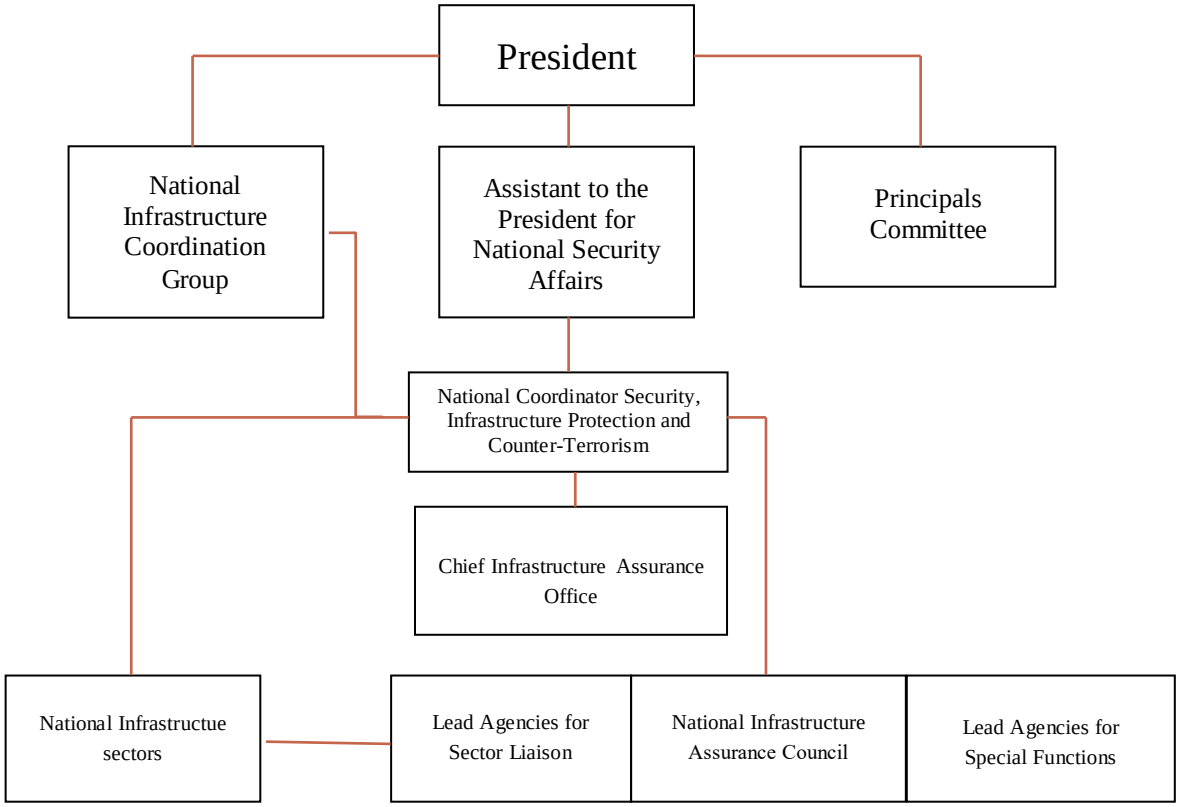

Fig. 1. *The chart (excerpt) of distribution responsibilities for national (critical) infrastructure protection according to Presidential Decision Directive PDD-63 (1998)*[8].

As shown on the chart above, the organizational structure built in pursuit of PDD-63 (1998) apparently reflected interconnection between CI protection and national security through assgning the relevant responsibility (including coordination at the federal level) to the competence of Assistant to the President for National Security Affairs.

Subsequently, especially in the aftermath of 9/11 and establishment of the *Department of Homeland Security (DHS*) interconnection had become complex including due to introduction of the term *homeland security*.

Paying attention to current trends in the security field it is worth to note that in 2018 a special body, the *Cybersecurity and Infrastructure Security Agency (CISA)* was

[8] Presidential Decision Directive (PDD NSC-63) May 22, 1998.
URL: https://fas.org/irp/offdocs/pdd/pdd-63.htm.

established within the DHS[9]. The CISA is an operative component of the DHS leading the national effort to understand and manage cyber and physical risks to national critical infrastructure.

1.2. The example of Germany

In Germany the term ***critical infrastructure*** is defined in the ***National Strategy for Critical Infrastructure Protection*** (2009)[10]:

> ***Critical infrastructures (CI) are organizational and physical structures and facilities of such vital importance to a nation's society and economy that their failure or degradation would result in sustained supply shortages, significant disruption of public safety and security, or other dramatic consequences.***

The definition presented above largely coincides with that in the U.S. legislation perhaps excepting a special emphasis placed on importance of sustainable supply of services and goods[11]. Also, the meaning of the term apparently reflects influence of CI conditions on *public safety* and *security* which apparently are recognized as components of *state security*.

According to the CIP Strategy, ***ensuring the protection of this infrastructure is a key function of security-related preparedness measures taken by industry and government agencies, and is a central issue of our country's security policy***.

As for an organizational and management aspect of the interconnection between CI protection (security) and national (state) security in Germany, the central national-level CIP measures are coordinated by *The Federal Ministry of Interior Building and Community (Federal MOI)*[12] the overarching responsibilities of which cover among others *public (state) security* including protecting the public against violence, crime, terrorism and activities intended to undermine German constitutional order.

The Federal MOI includes a number of specialized directorates and agencies to deal with Counter-Terrorism, Extremism, Organised Crime, to protect Public and Constitutional Law by means of carrying out the relevant policies through such subordinated to it agencies and centres as the *Federal Police, Federal Criminal Police Office, the Federal Institute "Technical Support Service"* and some others.

---

[9] The CISA was established after President D. Trump signed into law the Cybersecurity and Infrastructure Security Agency Act November 16, 2018, and charged with the leading role to play within U.S. Department of Homeland Security concerning protection of physical and cyber critical infrastructures and key resourced against terrorist attacks, natural or man-made disasters.

[10] National Strategy for Critical Infrastructure Protection (CIP Strategy), June 17, 2009.
URL: https://www.kritis.bund.de/SharedDocs/Downloads/Kritis/EN/CIP-Strategy.pdf.

[11] From authors' point of view, such an approach facilitates the analysis of infrastructure objects criticalilty and relevant objects assigning to the national CI.

[12] The Federal Ministry of Interior Building and Community.
https://www.bmi.bund.de/EN/ministry/structure-and-organization/structure-and-organization-node.html

As for CI protection, *the Federal Office for Civil Protection and Disaster Assistance* as well as the *Federal Office for Information Security* play key coordinating roles in this field being subordinated to the relevant directorates within the Federal MOI.

1.3. The example of Poland

According to the Polish *Act of 26 April 2007 "On Crisis Management*"[13],

> ***Critical infrastructure shall be understood as systems and mutually bound functional objects contained therein, including constructions, facilities, installations and services of key importance to the security of the state and its citizens as well as serving to ensure the efficient functioning of public administration authorities, institutions and enterprises.***

It is worth to note that today's Poland is a country whose political leadership tries to fastly respond to changes occurring in the security pattern both in global and in national dimensions. Thus, in recent years the Polish legislation concerning CI is in the process of a dynamic transfer from the concept of ensuring CI protection (security) to the concept of CI resilience as a component of national resilience. So, when further discussing the subject matter we should take into account both the close interconnection of these concepts and the transitional character of some legislative and regulatory acts in this field.

Below the brief overview of how links between CI protection and national security have been reflected in the Poland's legislation in recent years.

Following the basic for this field Act "On Crisis Management" we should note the governmental regulation on *National Critical Infrastructure Protection Programme* (30 April 2010)[14] approved in pursuance of the mentioned act.

Really, already §1 of the document declares that the regulation establishes "*the way of implementation of duties and cooperation in the scope of National Critical Infrastructure Protection Programme* ***by public administration authorities and services responsible for national security*** *with both sole and dependant owners and holders of buildings, installations, facilities and services of critical infrastructure, hereinafter ' critical infrastructure operators'* ".

In the context of the topic under consideration it is indicative that §3 of the regulation includes the provision that the "***Director of the Government Centre for Security*** with a view to compiling National Critical Infrastructure Protection

[13] ACT of 26 April 2007 on Crisis Management (consolidated text). Journal of Laws. 2013, 2015. URL: http://rcb.gov.pl/wp-content/uploads/WERYF_-ACT_Crisis_Management_English-1.pdf.

[14] 541 Regulation of the Council of Ministers of 30 April 2010 on National Critical Infrastructure Protection Programme. URL: https://rcb.gov.pl/wp-content/uploads/REGULATION-on-NATIONAL-CRITICAL-INFRASTRUCTURE-PROTECTION-PROGRAMME-AB.pdf.

Programme… shall develop the criteria…" enabling to distinguish the critical infrastructure within the systems."

The next important stage in development of the approaches to ensuring CI protection in Poland was connected with inclusion of a number of provisions addressing CI protection in the *National Security Strategy of The Republic of Poland*.[15] The document defines such strategic directions in the field of (national) security and Defense:

defensive actions;

protective actions;

social actions in the domain of security;

economic actions in the domain of security.

To illustrate the links between CI protection and national security we would like to underscore paragraphs 80 and 86 of section *3.2. Protective actions.*

According to paragraph 80,

> *The substance of protective actions is to ensure conditions allowing to* ***maintain constitutional order, integral stability of the state, public security and public order****, both common and individual tangible and intangible resources, as well as the* ***functioning of the critical infrastructure.***

Thus, we can see that protective actions with regard to CI are put in a line with those aiming at ensuring constitutional order, integral stability of the state, public security and public order.

Besides, according to paragraph 86 of the document,

> ***[I]t is extremely important to ensure conditions for the protection of critical infrastructure. The infrastructure comprises key systems and elements guaranteeing security of the state and its citizens****, as well as efficient functioning of public administration bodies, institutions and entrepreneurs.*

In terms of organization and management of the relevant activities, CI issues inclusion in Poland's security domain can be traced in a number of provisions of *The National Critical Infrastructure Protection Programme (NCIPP) (2015).*[16]

In particular, section *2.1.* of the mentioned document contains the statement that the NCIPP "… *is complementary to the* ***Strategy of development of the national***

[15] National Security Strategy of The Republic of Poland (2014).
URL: https://www.bbn.gov.pl/ftp/dok/NSS_RP.pdf
[16] The National Critical Infrastructure Protection Programme 2015.
URL: https://rcb.gov.pl/wp-content/uploads/NPOIK-2015_eng-1.pdf

security system of the RP 2022[17] *and* ***the Strategy of the National Security of the Republic of Poland*** *[2014]*.

In response to the recent changes in global security including those due to COVID-19 pandemy Poland approved new *The National Security Strategy of the Republic Of Poland 2020*[18] which makes assessment of the security environment of Poland as *"uncertain and unpredictable"* and "*hindering the pursuit of national interests and the achievement of strategic objectives"*.

In general, the document is evidence that essential changes have been observed in approaches to ensuring national security in Poland, and it requires a special in-depth-study. In the context of our discussion, it is worth to note that the new strategy focuses on ensuring Poland's ***readiness to respond to new challenges and threats and hazards through strengthening national resilience***, especially, ***by means of improvement of national security management*** and ***paying more attention to cybersecurity*** issues.

Really, the new Polish National Security Strategy underscores the role of communication systems recognized by the document as *"a key component of national security assets and preparatory measures for crisis situations and therefore they constitute an important element of the national critical infrastructure"*.

It should be expected that due to recent approval *The National Security Strategy Of The Republic of Poland 2020*, it is reasonable to suppose that certain changes will take place in approaches to CI protection in the country, but meanwhile all cited above documents remain in force.

More detailed reviews of the national approaches and practices show that, typically, links between CI protection (security) issues and national (homeland, state) security can be traced in national legislation already when defining the term *critical infrastructure.* But, even in case when these links are not formulated explicitly in a definition, they can be easily derived from consideration of functions and services provided by CI to maintain everyday life of people, reliable functioning of society and state institutions.

2. The review of legal frameworks and organizational forms in which the links between protection (security) of critical infrastructure and national (state, homeland) security reveal itself in three GUAM[19] member-states: Georgia, Moldova and Azerbaijan

[17] Strategy of development of the national security system of the RP 2022. URL: https://www.epicos.com/sites/default/files//strategy_of_development_of_the_national_security_system_of_the_republic_of_poland_2022.pdf .

[18] National_Security_Strategy_of_the_Republic_of_Poland_2020. URL: https://www.bbn.gov.pl/ftp/dokumenty/National_Security_Strategy_of_the_Republic_of_Poland_2020.pdf /

[19] In the GUAM states, Ukraine's partners in this international organization, the approaches for protecting infrastructure are implemented in such ways which for the purpose of this study are named as *fragmented* ones. As particular cases of such approaches implementation the national practices of some developed countries such as Germany and Austria can be assigned where measures aiming at ensuring CI

To gain a better picture of national approaches while considering a limited number of examples further we briefly analyze the national practices observed in three former Soviet republics, namely Georgia, Moldova and Azerbaijan, being Ukraine's partners within the framework of GUAM. Ukraine and these countries have much in common in their post-soviet history, including arms conflicts in their territories. Besides, all GUAM-members, at least during some periods of their recent histories made active attempts for approaching to EU and NATO memberships, but are still in the transition processes[20], among common peculiarities of which *is availability of serious security problems*.

4.1. The example of Georgia

The Internet search of either the term *critical infrastructure* or its synonym, *national infrastructure,* in English, Georgian and Russian[21] gave a zero result. Besides, whilst this report was being written there were no information and reports relatively to international forums, conferences, etc. where plans to establish a national CI protection system in Georgia be considered. Deriving from the above, one may say that the concept of CI protection is not implemented in the country.

At the same time, Georgia is on the list of the former Soviet republics which achieved considerable progress in implementing state-of-the-art approaches to cybersecurity. Really, according to *The Global Cybersecurity Index (GCI*) of *The International Telecommunication Union (ITU*)[22], Georgia ranks very highly in the European region and globally (9-th and 18-th positions, respectively). Interestingly, that contrary to the national legislation, some departmental documents addressing cybersecurity use the term *critical infrastructure.*[23]

One of the most important reasons of strengthened focus payed by Georgia to cybersecurity issues including protection of infrastructures vitally important for the country, were the lessons derived from the analysis of the relevant events occurred during the Russian-Georgian armed conflict in 2008. Really, according to Buckland, Shreier and Winkler from the Geneva DCAF[24],

---

protection (security) have been shaped in the important directions within cybersecurity measures rather than in establishing integral national CI protection systems.

[20] Author's opinions may not coincide with the governments' one on this issue. Really, according to the draft Development Concept «Azerbaijan – 2020: Outlook for the Future» published on President's site, "the transitional period has already ended in Azerbaijan."

[21] It is precisely these languages in which legislative and regulatory acts are published in the public domain in Georgia.

[22] Because of delay in Global Cybersecurity Index (GCI) 2019 publication resulted from COVID-19 pandemy hereinafter references are made to GCI 2018. (See Global Cybersecurity Index.
URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf).

[23] See, e.g., RFC 2350 CSIRT Description for CERT-GOV-GE.
URL: https://dea.gov.ge/uploads/Articles/CERT-GOV-GE%20RFC2350.pdf .

[24] Benjamin S. Buckland, Fred Schreier & Theodor H. Winkler Democratic Governance Challenges of Cybersecurity, DCAF HORIZON, Working Paper No.1, Geneva, Geneva Centre of the Democratic Control of Armed Forces, 2015 https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-

> "The cyber campaign against Georgia in August 2008 is the first example of cyberattacks that coincided directly with a land, sea, and air invasion by one state against another, and is probably the best example of how to properly employ computer network attacks in a modern battlespace.

Although the DCAF experts noted that the cyberattacks did not resulted in essential harm considering that the larger part of the national economy and infrastructure objects was beyond the cyberspace, yet due to the cyberattacks *during the most critical days of the battles the Russian media could present their vision on the armed conflict while the Georgian ones were actually cyberblocked*.

In Georgia, the direct links between security of those systems and objects which are usually assigned to CI in the most developed countries and national security issues are established in the Law of Georgia " On Information Security" through the definition of the term *critical information system* which means

> *[A]n information system whose uninterrupted operation is essential to national Defense and/or economic security, as well as to normal functioning of the state authority and/or society.*[25]

4.2. The example of Moldova

The publicly available information concerning CI protection in the Republic of Moldova has a character similar to that of Georgia, namely – the country has made significant efforts aiming at improvement of its cyberpsecurity under influence and with support of the NATO and EU member-states. Really, according to the last publication of the GCI[26] of the ITU the RM occupies 31-st and 53-d ranks in the European and global rankings, respectively.

One could witness the similarities in Moldova with the processes observed in Georgia in the following facts: "*The national strategy on a digital society development "Digital Moldova 2020*" approved by the governmental decree in October 2013 section *4.3. Protected and secured digital environment* put inter alia a specific objective — *improvement the lelel of cybersecurity of the critical national infrastructures (state authorities/institutions, communication networks, water pipelines, power systems, transport systems, etc.).*

Section 4.3 of the document also includes the provision concerning the need to identify national critical infrastructures to be protected against cyberattacks.

Again, basing on publicly available information it may be concluded that at the

https://www.dcaf.ch/sites/default/files/publications/documents/Horizon_1_Good_Governance_CyberSecurity_RUS.pdf .

[25] Law of Georgia "ON INFORMATION SECURITY" (2012), https://matsne.gov.ge/en/document/view/1679424?publication=3

[26] Ref. to note 22.

moment the above mentioned objective was withdrawn from the nation's agenda, since neither national legislation nor governmentals plans[27] have mentioned CI protection (security)[28]

At the same time, the widespread use of a concept *infrastructure* in all areas of activities in Moldova may be considered as a specific feature of nation's governance mechanism. Really, the concept *infrastructure* is used in the largest range of activities beginnign from military and IT-domains to sport and cultural objects and systems.[29]

The case of Moldova shows that the national government clearly understands the links ***between cybersecurity and national security***, and such awareness is reflected, for example, in the governmental plan for 2020 – 2023[30], in which cybersecurity issues may be found in Section XI. *Security and Defense*.

4.3. The example of Azerbaijan

In the context of the topic under consideration, ***Azerbaijan has focused on security of its infrastructure related to energy carriers extraction, production and transportation***, reducing the vulnerability of the relevant infrastructures to natural disasters and acts of terrorism and sabotage. In particular, the relevant provisions are included in *the Law of Republic of Azerbaijan "On National Security"* (2004)[31]

Exploring open-source information allowed us to conclude that ***there were no terms critical infrastructure*** or its equivalent***, national infrastructure,*** in legislation of Republic of Azerbaijan. Again, only some documents relating to cooperation between Azerbaijan and NATO contain the term *critical infrastructure,* when it comes to cooperation with the Alliance in the field of *critical energy infrastructure security*, in other words, when addressing security of CI's fragment.

According to Institute of Information Technologies of the National Academy of Sciences of Azerbaijan, as of 2 March 2020, work was continued to develop the draft *"National Strategy of the Republic of Azerbaijan on Information Security and Cybersecurity for 2020 – 2025"* with support of the relevant European and NATO structures.

National legislation of Azerbaijan and official documents relating to cooperation of Azerbaijan with the EU and NATO demonstrate that ***the political leadership of the country is clearly aware of interlinkages between critical energy infrastructure security and national security***.

---

[27] For example, see, *Plan deistviy Pravitel'stva na 2020 – 2023 gody* (*The Governmental Working Plan for 2020-2023*). URL: https://gov.md/sites/default/files/document/attachments/pag_2020-2030-ru.pdf.

[28] However, information about plans of Moldova's representatives to participate in the international forum in Romania (October 2020) devoted to CI protection may be considered as a hint of possible changes in this field.

[29] In total, *The Governmental Working Plan for 2020-2023* contains references to 17 infrastructures.

[30] Ref. to note 27.

[31] "On National Security": The Law of the Republic of Azerbaijan № 712-IIQ of 29 June 2004. URL: https://www.legislationline.org/download/id/5410/file/CODEXTER%20Profile%202014%20Azerbaijan.pdf.

3. Implementation of a critical infrastructure protection concept in terms of maturity of national security and defense sector management mechanisms

As the preceding sections of the present report show, in the world today awareness of necessity to protect critically important for each state infrastructures does not always lead to establishment of integral CI protection (security) and resilience systems.

Sometimes, even if perception of threats and related risks to CI is adequate, it may be insufficient for practical implementation of an integral national (state) CI protection system.

Really, relevant decisions approval and implementation also may depend on a number of factors resulted from, inter alia, national economy transitional conditions, unfavourable security environment (e.g. armed conflict consequences) and ***the factor of management mechanisms maturity*** in the national security and defense sector.

An analysis of both CI protection concept implementation and necessity to build an integral CI protection system from a management standpoint makes it possible to highlight some specific features of this process, and under certain conditions to evaluate related objectives in terms of their timeliness and given priorities

Below, when discussing an issue, we shall rely upon a number of obvious assumptions and facts. They are the following:

1. The developed countries sharing the principles of democracy and market economy have, as a rule, the mature mechanisms of state management.

2. The national security and defense sector management mechanisms are specific ones being at the same time, integral parts of a state management process as a whole.

3. Establishment of integral state (national) CI protection systems (application of *integral approaches*[32]) is typical for the developed countries.

4. Reaching the state of maturity of management mechanisms, in particular, in a national security and defense sector, is a time-consuming process with its stages to be implemented, as a rule, in a certain order.

5. As for developing countries and those being in transitional preriods including because of influence of unfavourable security conditions, *the fragmented approaches*[33] *are usually applied* to protect important infrastructures. Such approaches, under certain conditions, may be considered as *early stages for application of integral*

[32] For the purpose of the given report an *integral approach* means such an approach which is implemented to protect critically important for people, society and state institutions objects and systems through establishment of the national critical infrastructure protection (security) and resilience system.

[33] For the purpose of the given report, the *fragmented approaches* means such approaches applied to ensure protection (security) and resilience of infrastructural objects and systems under which relevant security and resilience measures are taken within the frameworks of individual security domains (e.g. cybersecurity, energy security, etc.)

approaches.

Relying upon the above assumptions it may be supposed that ***the transition to a qualitatively new level of management required to implement a CI concept and to establish a national CI protection system must go hand in hand with efforts undertaking to reform State management mechanism as a whole***. It would be an error to assume that it is possible to ensure execution of proper procedures for coordination, cooperation and sharing information within a reformed individual domain leaving others unreformed.

This does not necessarily mean that all stakeholders (we are saying about CI protection system establishment[34]) shall wait for some special messages to start reforming. Under favorable conditions, the progress achieved in this particular security domain might serve as a driver for reforming the national security and defense sector as a whole.

Basing on the above, therefore, it is important to identify priorities in planning the reforming process in order to set its stages and a reasonable consequence of their implementation.

From that standpoint, one of the important stages which results should be taken into account in a prioritizing process is ***the maturity assessment for available management systems in related security domains***. Such an assessment shall include finding the answers to the following questions:

Is there awareness of final goals to be achieved by means of reforming?

Are there in place necessary conditions to launch a process?

The answer to the second question implies that when reforming existing systems and establishing new ones, decision makers are aware of necessity to follow a proper sequence of stages implementation. The typical stages for security system establishment are presented below.

[34] See Governmental order "On approval of the Concept of establishment of the State system for critical infrastructure protection" (Pro shvalennya Kontseptsii stvorennya derzhavnoi systemy zahystu krytychnoi infrastruktury), Rozporyadzhennya Kabinety Ministriv Ukrainy № 1009-p vid 6.12.2017 r.
URL: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#Text

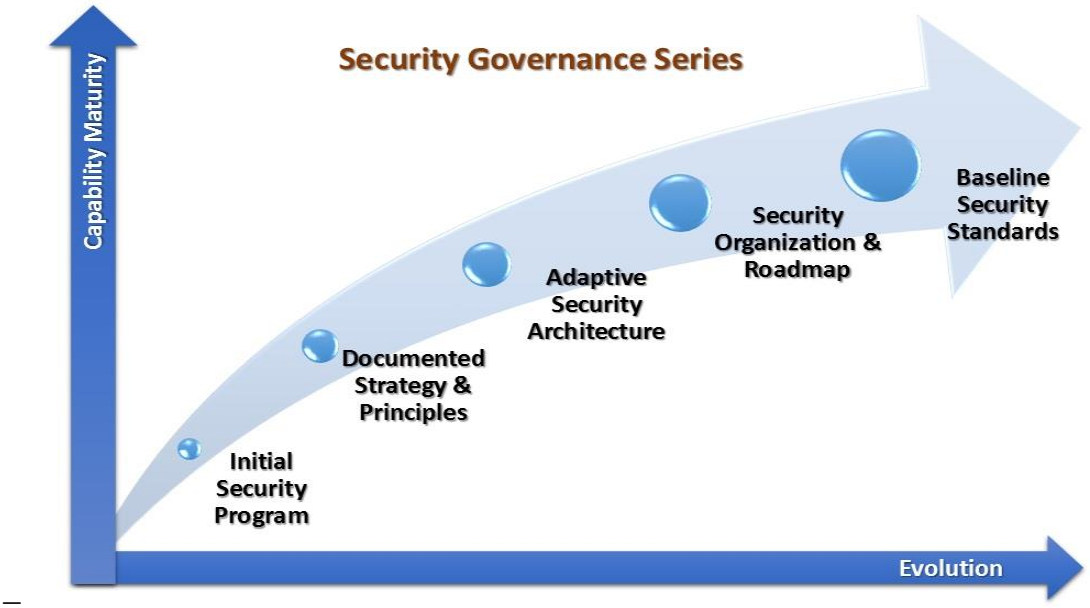

Fig. 2. The typical model stages in the process of security system establishment)[35].

Bearing in mind the examples of the national practices outlined above concerning links among national (homeland) security, CI protection (security) and cybersecurity it may be concluded the following:

The most developed countries and international organizations uniting such countries[36], as a rule, implement the CI protection concept and give priority attention to direct relationship between CI protection and national security issues.

As for other category of countries to which we assigned the former Soviet republiscs, nowadays GUAM member-states (Georgia, Moldova, Azerbaijan), having much in common: transition characters of their economies; frozen armed conflicts[37] in their territories; and a relatively high level of cooperation with European and Euro-Atlantic structures; *the fragmented approaches to ensure security of infrastructure objects and systems* are applied by the GUAM member-states with some peculiarities deriving from specificity of security and economic conditions for each country.

To be more specific, in the above countries the undertaken measures to protect infrastructure objects and system have been implemented within the frameworks of efforts aiming at achievement of an appropriate level of either cybersecurity or energy

[35] Project RECIPE 2015. Resilience of Critical Infrastructure Protection. Guidelines. URL: https://ec.europa.eu/echo/sites/echo-site/files/recipe_guidelines.pdfhttps://ec.europa.eu/echo/sites/echo-site/files/recipe_guidelines.pdf.

[36] The authors mean primarily the member-states of NATO, EU and OECD (Organization for Economic Cooperation and Development). In this context, such countries as Germany and Austria may be considered as exceptions because in their national legislations the term *critical infrastructure* is defined, their authorities maintain the lists of CI objects and systems but the relevant efforts are implemented around the pivot activities aiming at ensuring CI cybersecurity.

[37] The Ukrainian version of the analytical report was published in July 2020, several months before the "frozen" conflict around Nagorno-Karabakh erupted again.

infrastructure security[38], while the relevant directions of activities are clearly recognized as related to national security.

Such a pattern of CI and its protection (security) and resilience concepts in different countries allows to supposing that the full-scale implementation of the above mentioned concepts is typical for the developed countries, having mature mechanisms of State governance, in particular in national security and defense domains, as well as sufficient financial and economical capabilities.

Therefore, when determining whether reforming security systems is necessary (in this context we mean systems related to CI protection and resilience), which reforming models are feasible, what are the durations and consequences of possible working stages, etc. ***it is increasingly important to assess the maturity of related systems (mechanisms) of State governance.***

Reviewing open-source information on this particular topic does not give us references to examples of using such an approach to CI protection as a whole but some results are available in the cybersecurity domain. Familiarising with the above mentioned results indicates that *the methodology used for assessing the maturity of State cybersecurity systems may be extended to the CI protection (security) and resilience domain almost without exceptions.*

Similarly to the cybersecurity domain (with proper corrections), when assessing the maturity of a system designed to ensure CI protection (security) and resilience the key answers should be received regarding availability of the following:

1) ***oficially approved national strategy to ensure CI protection (security) and resilience*** (legislative foundations for the State policy in the CI security domain);

2) ***officially defined authority charged with responsibility for CI protection (security) and resilience*** as well as coordination of relevant activities at the national level.

3) ***national structure (network) charged with gathering, processing and sharing information*** on security incidents (crises) involved CI;

4) ***formally approved program aiming at interdepartmental cooperation concerning CI protection (security) and resilience***;

5) ***formally approved program of the public-private partnership in CI protection (security) and resilience*** domain.

Of course, a thorough analysis of the maturity factor may not be restricted with finding the relevant facts only, nevertheless these facts play a key role since deriving from them the conclusion can be made on the basic elements of the CI security architecture presence/absence providing for CI functioning.

[38] The experience of the GUAM member states indicates that cooperation of these countries with the NATO and EU has played a decisive role in inclusion of infrastructure security issues in the national governments' agendas.

4. The attempted implementation of the CI and its protection concept in Ukraine: finding the model to integrate CI protection in the national security domain?

In the preceding sections of the report the role and place of activities aiming at ensuring CI protection (security) and resilience within the national (homeland) security domain have been analyzed by the authors basing on the experience of some foreign countries.

When doing so, not only the approaches and practices typical for the developed countries in which high levels of management mechanisms maturity have been achieved but the national practices of the countries being in transitions periods and in the complicated security conditions as well.

On the basis of presented above observations an obvious conclusion can be made that countries in different political, security, economical and other conditions may use significantly different approaches to protect critically important objects and systems. And, from our standpoint, ***one of the key factors having substantial influence on the choice of one infrastructure protection model (architecture) or another and related activities trajectories, is the level of maturity of the State governance mechanisms in the national security and defense domain***. This is particularly evident when analyzing management (governance) mechanisms in terms of responding to crisis situations.

From our perspective, finding an answer to the question, ***why the national level decisions on CI protection system establishment in Ukraine are not implemented yet*** (or considerably delayed)**,** is a necessary precondition for further meaningful steps towards achiement of the goal – to ensure CI protection (security) and resilience.

Thus, these steps should be based on the analysis of factors which had prevented implementation of the decision of the National Security and Defense Council of Ukraine of 29 December 2016 "On improvement of measures to ensure the protection of critical infrastructure objects" put into effect by the Decree of President of Ukraine №8/2017.[39]

4.1. The brief analysis of the attempted implementation of the decision of the National Security and Defense Council of Ukraine on critical infrastructure

Despite the fact that in the above NSDCU's decision the issue of ensuring critical infrastructure security was related to the priority directions of State policy in the national security domain, among the objectives set by the decision the only one was fully implemented, namely the development of the draft Concept of establishment

[39] On the decision of the National Security and Defense Council of Ukraine "On improvement of measures to ensure the protection of critical infrastructure objects", the Decree of President of Ukraine" №8/2017 of 16 Jan 2017. https://zakon.rada.gov.ua/laws/show/8/2017 .

State CI protection system (hereinafter referred to as the *Concept*) and its approval by the Government.[40]

Besides, the Concept was approved by the Government only in December 2017[41] (nearly 9 months late). The process of the draft Law of Ukraine "On critical infrastructure and its protection" also was carried out slowly. One of the reasons for it, in our view, was the absence of a shared vision of high relevance of the law and its objectives among the participants of the working group established under the Ministry of Economical Development and Trade of Ukraine. Eventually, in May 2019 the draft law was introduced late in the Verkhovna Rada.[42]

The previous Ukrainian Parliament did not considered the drat law. Later, in connection with election of new parliamentarians and a new Government appointment the draft law was withdrawn from the Verkhovna Rada.

At this point, it is important to highlight that the final version of the draft law had a number of terms and provisions which differ from the objectives formulated in the above NSDCU's decision.

NISS' representatives involvement in the above outlined activities allows us to suggest that in the process of the draft law development and its provisions alignment, ***ministries and other agencies efforts were mainly aiming at promotion the provisions of the draft law reflecting the short-term departmental interests,*** while implementation of the CI protection concept requires creation of new supra- and interministerial (departmental) mechanisms of management, and providing, at least at the first stages, efficient coordination, cooperation and information sharing among security and crisis response systems in place.

During the working group discussions around draft law provisions a number of participants maintained a position that all issues associated with security of infrastructure objects including procedures for coordination, interaction and sharing information had already been settled within the existing state systems.

As for this argument, we could only agree that vitally important objects and systems in Ukraine, just as in other countries, have always been primary concerns of the governments, authorities and other actors in this field. But, whether it is sufficient to argue that within the existing systems measures taken to ensure CI protection

[40] The excerpt from NSDCU's decision (unofficial translation): "2. within two months after approval of the Concept of establishment the State critical infrastructure protection system with the participation of the Security Service of Ukraine, the Foreign Intelligence Service of Ukraine and the National Bank of Ukraine to draft the law of Ukraine "On critical infrastructure and its protection" and according to the prescribed procedure to submit the draft law to the Verkhovna Rada…" (See Presidential Decree №8 of 16 Jan 2017.

[41] Order of the Governmental of Ukraine. "On approval of the Concept of establishment of the State system for critical infrastructure protection" (Pro shvalennya Kontseptsii stvorennya derzhavnoi systemy zahystu krytychnoi infrastruktury), Rozporyadzhennya Kabinety Ministriv Ukrainy № 1009-p vid 6.12.2017 r.
URL: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#Text

[42] The Verkhovna Rada received the draft law 27 May 2019 (almost two years late). See: Proekt Zakonu pro krytychnu infrastrukturu ta ii zahyst. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=65996).

(security) and resilience are adequate to current challenges and threats to which Ukraine?

It was shown in a number of NISS studies that ***in the absence of a state (national) system designed to ensure CI protection (security) and resilience the relevant objects can not be adequately protected by the security and crisis response systems existing in Ukraine,*** especially in case complex threats resulting in large scale crises.[43]

Really, in Ukraine, the objects which are usually assigned to CI in other countries, are divided into more than ten separated categories. Below, only part of them is presented:

- *enterprises of strategic significance for economy and national security;*
- *vital assets in the energy sector;*
- *vital assets in the oil and gas sector;*
- *assets to be protected and defended in emergency and under special periods;*
- *potential targets for terrorists;*
- *high hazard facilities;*
- *radiation-hazardous facilities; etc.*

Various authorities are charged with responsibilities for their security and safety and for relevant national (state) systems functioning. Besides, each national system has its "own" sets of threats and risks to be addressed, "own" modes of functioning under different security and safety conditions, "own" plans and procedures for responding outlined in departmental terms and concepts.

In addition, the situation has been exacerbated by the fact that the mechanisms and procedures for cooperation, interaction and information sharing among the existing systems even if available in relevant plans, have not been properly tested and validated for large scale crises because the practice of interagency drills and trainings has not been developed well enough restricting, as a rule, with those of a facility level. ***While, it is clear, that the main purpose of systems designed to ensure CI protection (security) and resilience is to prevent large scale crises and to respond to such crises when they do occurs.***

The situation around CI concept introduction in Ukraine was changed quite dynamically, and the standpoints of the Ukrainian ministries and other authorities evolved influenced with complicated security processes both outside and inside the country. In a number of important areas the idea of establishment a national CI protection system over a certain period of time was being supported by the Ukrainian law enforcement and security agencies, among which the Ministry of Internal Affairs

[43] *Developing The Critical infrastructure Protection System in Ukraine*: monograph / [S. Kondratov, D. Bobro, V. Horbulin et al] general editor O. Sukhodolia. – Kyiv: NISS, 2017. -184 p.

(MIA), Security Service of Ukraine (SSU) and State Service of Special Communication and Information Protection of Ukraine (SSSCIPU).

For example, the MIA created a profile structural unit on CI protection issues, the SSU strengthened the counterintelligence protection of CI, and the SSSCIPU was actively cooperating with other organizations to use the opportunities for synergy between the CI protection system and the Cybersecurity national (state) system.[44]

Nevertheless, the process of drafting the law was contradictory and inconsistent. A number of the Ukrainian authorities failed to go beyond their narrow departmental interests, and the final version of the draft law has been heavily criticized, among others, by the private sector representatives.

Taking into account the management maturity factor makes it possible to consider the process of CI protection concept introduction in a somewhat different way. When doing so, we can make an assessment on prioritization and timeliness of some objectives mandated by the relevant NSDCU's decision.

In addition, when discussing the subject matter we should keep in mind that to a certain extent suspicious attitude of some Ukrainian agencies to the plan of CI protection system establishment has been formed, at least partly, with a number of previous failed reforms of the State apparatus and their contradictory results.

Basing on the above considerations, resulted from the analysis of the situation around CI concept introduction in Ukraine, the authors believe that ***unacceptable delay in drafting and approving the profile law and establishing a State CI protection system is a result of management mechanisms immaturity rather than deliberate blocking implementation of the objectives defined in the above mentioned decision.***

Therefore, for the countries considered in Section 2 in which the levels of State management have not achieved the standards typical for the developed countries, it is hardly a coincidence that these countries apply *fragmented approaches* to vital infrastructure objects protection. It may be suggested that insufficient maturity of the State management mechanisms is both directly and indirectly derived from the fact that the national economies of these countries are in transition states, while their national security and defense sectors are subject to a distorting impact of severe security conditions.

[44] When the English version of the analytical report was being prepared, the positive developments revealed in establishment of a regulatory framework, which can serve as a common for the *fragmented approach* and *for integrated* one, and the authors decided that it would be useful to briefly familiarize English speaking readers with these updates. Really, thanks to efforts of the SSSCIPU supported by the NISS at the expert level, recently the Ukrainian Government approved the two important resolutions related to protection of the critical information infrastructure and critical infrastructure protection (see Anexes 1 and 2 which are additional in comparison with the original Ukrainian version of the report).

At the same time, despite the serious progress achieved, the level of management mechanisms maturity in the national security domain is still insufficient to implement the full scale CI protection (security) and resilience system (*integrated approach*).

4.2. The maturity assessment for the existing in Ukraine systems designed to ensure security of the objects to be assigned to CI

If we try to assess the maturity of the Ukrainian systems designed to ensure security of the objects which in developed countries are, as a rule, assigned to CI, ***directly expanding to CI security domain the approach already used to assess the maturity of the national cybersecurity systems*** (see the list of the questions from *a.* through *e.* in Section 3), the results will be expected.

Really, Ukraine started establishing the State CI protection system only in 2016-2017, and has fully completed the only objective from those defined in the NSDCU's decision, namely – development and approval of the Concept for establishing the State CI protection system. Whereas the remaining answers show that there are no additional indicators (elements) typical for a mature management system in this particular domain.

The same conclusion will be made using the approach illustrated by Fig. 2, supposing that in our case a security system is a State CI protection system. According to the chart presented the sequence of stages recommended for security system establishment, Ukraine has implemented only the first and the second (partly) objectives.

Besides, in this context the specifities of the situation around the CI concept introduction in Ukraine include the following: after the stagnation period in the national security domain significant time has been spent for raising the awareness of urgency of the CI protection issues and obtaining the proper expert support to bring these problems to the highest political level.

Thus, summarizing the above considerations we can assert that ***the reasons for considerable delay in CI concept introduction in Ukraine have a systemic character rather than a random one, and are largely due to insufficient maturity of management mechanisms in the national security and defense domain.***

4.3. The options to ensure protection (security) and resilience of CI objects in Ukraine

The conclusion on ***the natural character of the delay in implementation of the objectives identified by the relevant normative instruments on CI in Ukraine, leads us to the recognition of the need for a clearer trajectory*** determination towards ensuring CI protection (security) and resilience in Ukraine. It is obvious that after the draft Law of Ukraine "*On critical infrastructure and its protection*" had been *withdrawn from Verkhovna Rada, we can state that in tackling CI protection problems a considerable uncertainty has emerged.*

Really, the recommendation for draft revision by the new Government required for the second draft law submission to Verkhovna Rada, has seen slow implementation, and, again, one of the reasons to be mentioned, is, in part, lack of

clear awareness of urgency the issues to be addressed by the law and these issues direct relationship with national security problems. Others are apparently connected with current increasingly complex and rapidly changing social, political and economic conditions in Ukraine.

At the same time, infrastructure objects security and resilience continue to be included in the national governments' priorities worldwide. In addition, it is apparent, that the lessons drawn from the analyses of crisis responding to the pandemy of COVID-19 will be a basis for setting new goals and objectives concerning development of mechanisms and tools designed to ensure national infrastructures functioning under emergencies similar to those emerged in cases of COVID-19 quarantine restricitons imposing and lifting.

While Ukraine has significantly slowed the process of CI protection concept implementation, a new tendency is being observed in the most developed countries, namely ***they are paying more and more attention for resilience of carrying out vitally important functions and providing critically important services to ensure the national resilience.***

This means that a new stage in development of security approaches has been already started during which the roles of authorities, private sectors, peoples and other actors will be strengthened within the framework of the process aiming at ensuring CI protection (security) and resilience as one of the basic components of the national resilience.

4.4. Some preliminary observations concerning the lessons learned from the early stages of responding to COVID-19 pandemic in Ukraine

The experience gained in responding to COVID-19 pandemic in various countries has shown that even where the CI protection (security) and resilience systems were in place due to an unprecedented scale of the crises, national governments faced huge problems, in particular when determining those objects and systems which had to continue their operation under quarantine restrictions, as well as when the need arose to resume gradually and/or alternately such objects and systems operation.

As for Ukraine, the preliminary analysis has indicated that ***by the beginning of COVID-19 pandemic in a number of domains Ukraine had no efficient tools, technical and organizational capabilities as well as sufficient resources to adequately respond to this imminent threat*** (for more details ref. to publication [45]). Therefore, the most of the complicated decisions (including on imposing the

[45] *Deyaki problemy reaguvannya na poshyrennya COVID-19 u konteksti zabezpechennya bezpeky ta stikosti krytychnoi infrastruktury*; (Деякі проблеми реагування на поширення COVID-19 у контексті забезпечення безпеки та стійкості критичної інфраструктури): аналіт. зап.
URL: https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/deyaki-problemi-reaguvannya-na-poshirennya-covid-19-u-konteksti .

quarantine) the Ukrainian authorities approved directly during the responding to the crisis situation, which affected the quality and consistency of measures taken, and required follow-up corrective actions, etc.

Despite the large scale and uniqueness of problems connected with response to COVID-19, it is quite apparent that a number of tasks emerged might be solved more rapidly and effectively if Ukraine had laid the foundation of a CI protection system not to mention about either such a system or its essential components available (for more details ref. to publication[46]).

Actually, ***ensuring operation of a CI protection system includes, inter alia, development and maintenance of the national list (register) of objects and systems assigned to CI, determination of their operation modes under various security and safety conditions***, etc.

It is clear, if the relevant legislative and regulatory acts had been available by the beginning of COVID-19 pandemic it would be much easier to plan and implement necessary measures (in particular, imposing/cancelling quarantine restrictions). Such legislation would serve as a firm foundation in a decision-making process and in solving operative tasks emerged during responding.

It is well known that responding to global events similar to COVID-19 pandemic requires, inter alia, a new higher level of coordination, interaction and information sharing (CIIS) among state and local authorities, businesses, people, other actors, aiming among others to mobilize all available resources nationwide, taking into consideration potential cascade and domino effects, etc. Whereas, it is creation of national (state) CI protection (security) and resilience systems that includes establishment and cardinal improvement of the CIIS procedures involving all actors, as one of the main direction of relevant efforts.

Thus, turning to the problems of CI concept implementation in Ukraine, we can state the following:

> ***If our country has strategic plans to be among the most developed nations relying upon market economy and State management basing on democracy principles, then there are no rational alternatives to move further in order to ensure CI protection (security) and resilience.***

One of the consequences of the above statement acceptance should be clear understanding that ***our country will not be able to successfully reform the national security and defense sector without recognition of CI protection (security) and resilience issues as an intergral part of national security domain,*** and, eventually,

[46] *Stiykist' krytychnoi energetychnoi infrastruktury: svitovyi dosvid funktsionuvannya energetychnykh kompaniy v umovakh poshyrennya COVID-19* (Стійкість критичної енергетичної інфраструктури: світовий досвід функціонування енергетичних компаній в умовах поширення COVID-19): аналіт. зап.
URL: https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/stiykist-kritichnoi-energetichnoi-infrastrukturi-svitoviy-dosvid

this provision must be reflected in all relevant mutually agreed conceptual and strategic documents as well as in the national legislation.

Thus, in the near future it is necessary to decide on the national level, which steps should be taken in terms of providing organizational and legislative basis to resolve the problems of CI protection (security) and resilience.[47]

From authors' standpoint, when answering this question ***we should unambiguously exclude all options resulting in keeping beyond the political leadership's attention the modern trends in protection national CI in one way or another against all cyber- and physical threats***.

From the above, ***the situation around establishment of the State CI protection system urgently needs to be analyzed***.

When analyzing, it is necessary to examine in detail the experience and practices of a wider circle of countries including the GUAM member-states, which currently are implementing the *fragmented approaches* to ensure protection of their infrastructures.

The authors believe that at this stage ***the more promising would be a conclusion on necessity and possibility to apply an integral approach for building the State CI protection (security) and resilience system basing on the experience and proven practices used in the developed countries*** (first of all, in the NATO and EU member-states).

To organize of follow-up work in this direction a clear working plan should be developed providing special managerial measures to overcome systemic obstacles which, inter alia, prevented to develop and approve the profile legislation in due time, with further specific steps from the law to its practical implementation.

Meanwhile, in the current global turbulent security and economical conditions, we should not categorically reject other options, for example, a phased establishment of a CI protection (security) and resilience system. When so doing, *a fragmented approach* may be recognized as the first phase of the process aiming at *an integrated system* creation.

The review of foreign experience and practices in this security domaing clearly shows that whatever course selected addressing vitally important objects and systems protection (security) and resilience, ***the urgent tasks will certainly include the development and maintenance of an objects list (register),*** which, in turn, requires the ***development and approval of methodologies and procedures to assign infrastructure objects to the above list (register)***[48].

[47] Of course, the answer to this question may not be separated from general strategic planning process in the national security domain.

[48] The tasks have been implemented by the moment of publication of the English version of the report (see Annexes I and II).

Successful achieving of the above objectives is impossible without getting awareness of a role played by CI in stable, safe and secure functioning of a modern State. Thus, the hope is that implementation of a CI protection concept in Ukraine will considerably contribute to the reform process both of State management, in general, and national security and defense sector, in particular.

Therefore, recognition of CI protection (security) and resilience issues as ones belonging to national security domain will require further steps to ensure agreed policy in this field, including updating and harmonizing a number of strategical and conceptual documents.

Currently, in connection with the considerations presented above, of special interest are efforts to introduce *a national resilience concept* in Ukraine. Such efforts are in line with the widely recognized contemporary approaches in the field of national security, and we support them.

At the same time, it should be noted that earlier in this report we have addressed to a certain extent the correlation between *resilience* and *security* terms relating to CI issues. In this context, it is important to underscore that all ***foreign experience and practices in this field shows that implementation of the CI protection concept historically preceded CI resilience one***. Bearing in mind this consideration, from authors' standpoint, it would be reasonable to carry out a special study to examine the potential impact of the maturity factor on the management mechanisms in the national security and defense sector before practical steps will be taken to build the national resilience system.

The conclusions and recommendations

The work on this report was carried out against the background of dramatic and ambiguous processes affecting cardinally the security environment in global, regional and national dimensions.

The most of these processes are connected, in one way or another, with national governments' (and sometimes, specialized international organizations') capabilities and competences to evaluate threats, hazards and related risks of potential crises (emergencies of various natures) and to respond to such crises providing, as far as possible, people safety, stable operation of State's and society's institutions, etc.

It is the above mentioned security and safety aspects that are largely determined by existence of national CI protection systems, their efficiency and resilience. C

Similarly to the situations around the nuclear power in the post-Chernobyl era and counterterrorism activities after 9/11 attacks when global revisions of relevant approaches and standards were made, the serious lessons have been and will be learned from responding to COVID-19 pandmemic and related with it unrests in the U.S. and other countries.

Basing on the above considerations presented in this report, from authors' standpoint, it is necessary to conclude the following:

1. For the most national governments of the developed countries the goal to ensure the stable operation of objects and systems vitally important for everyday life (***critical infrastructures***), due to which peoples, State and public institutions, etc. have access to key resources and critical services, ***remains among the priorities in the national (homeland) security domain.*** Therefore, there is a need to recognize

2. The review of foreign experience and practices in this field shows that the objectives and tasks derived from the above mentioned goal are largely achieved through implementation of a CI concept. At the same time, due to specifities of conditions (first of all, security and economical) in which different countries are, and depending on the maturity of State management (governance) mechanisms these objectives and tasks are achieved using different approaches which can be provisionally divided into two main categories:

A. ***Integrated approaches*** (typical for the developed countries, first of all, EU and NATO member-states)**:** within the frameworks of such approaches State CI protection (security) and resilience systems are established to withstand all cyber- and physical threats;

B. ***Fragmented approaches*** (typical for countries being in transition conditions where the levels of State management are essentially lower than those in developed ones): within the frameworks of these approaches national governments to ensure protection and resilience of important infrastructures take necessary measures around a separate security direction (e.g. cybersecurity, energy security, etc.). Under certain conditions the *fragmented approach* can be considered as the first stage in the process of *integrated approach* application.

3. The analysis of establishment of the CI protection system in Ukraine makes it reasonable to assumet that the main reasons for failure to implement NSDCU's decision had a systemic character and largely arose from insufficient maturity of management mechanisms and procedures in the national security domain.

4. The results of the preliminary review of lessons learned from responding to COVID-19 pandemic both worldwide and in Ukraine have underscored a high priority of CI operation issues.

5. To date, there is an urgent need for intensifying State policy to ensure CI protection (security) and resilience in Ukraine.

On the basis of study carried out and bearing in mind the above conclusions, we consider it useful ***to recommend the following***:

1. ***The Cabinet of Ministers of Ukraine*** should:

1.1. Present to the Verkhovna Rada the revised draft Law of Ukraine "On Critical Infrastructure Security and Resilience".

1.2. Develop and approve the procedures for assigning objects and systems to critical infrastructure.[49]

1.3. Ensure the critical infrastructure register establishment and maintaining.

(On completion of this point it will be possible to reframe further steps in order to apply an integrated approach providing for State critical protection system establishment).

1.4. Develop and approve the National critical infrastructure protection plan.

2. **The Staff of the National Security and Defense Council of Ukraine** should:

2.1. Prepare and submit to the Council meeting the matter of recognizing critical infrastructure protection (security) and resilience as one of the directions of ensuring national security which will require proper amendments to the Law of Ukraine "On national security of Ukraine";

2.2. Consider the possibility to establish a temporary interagency working group on critical infrastructure security and resilience charged with providing integrated support of establishment the State system for critical infrastructure security and resilience.

2.3. Examine the progress in implementation of NSDCU's decision "On improvement of measures to ensure the protection of critical infrastructure objects" entered into force by the Decree of President of Ukraine" № 8/2017 of 16 Jan 2017, within the framework of exercising NSDCU's oversight functions relating to its decisions.

[49] The recommendation has been implemented by the moment of publication of the English version of the report (see Annex II to this report).

Annex 1

The summary of Resolution №943 of the Cabinet of Ministers of Ukraine
"On certain issues of the critical information infrastructure"[50]
adopted on October 9, 2020, Kyiv

The resolution has been adopted by the Government in pursuance of Article 4. *The objects cybersecurity and cyberprotection* of the Law of Ukraine "*On basic principles of ensuring cybersecurity of Ukraine*" on October 9, 2020. The document was submitted to the Cabinet of Ministers by the State Service of Special Communications and Information Protection of Ukraine (SSSCIPU).

In accordance with paragraph 1 of resolution the two following regulations have been enacted:

1. *The procedure for drawing up the List of the critical information infrastructure objects;*
2. *The procedure for the inclusion of critical information infrastructure objects in the State register of critical information infrastructure objects, its drawing up and operation.*

In accordance with paragraph 2 of the resolution the SSSCIPU was entrusted to draw up the *List of the critical information infrastructure objects* and to submit it to the Government according to the established procedure. Besides, the SSSCIPU was charged to develop a form for submitting information to the *State register of critical infrastructure objects.*

In line with paragraph 3, the ministries and other executive authorities within six months should:

- draw up the sectoral lists of the critical information infrastructure objects being in their operation;
- provide these lists maintenance; and
- submit to the SSSCIPU relevant information about critical information infrastructure objects.

In accordance with paragraph 4, Government's resolution №563 (August 23, 2016) establishing the procedure of drawing up the list of information and telecommunication systems of the objects of State critical infrastructure, has been repealed.

The procedure for drawing up the List of the critical information infrastructure objects attached to resolution №943, establishes the mechanisms for drawing up the national and sectoral lists of the critical information infrastructure (CII) objects. In addition the document defines a number of important terms relating to the security of the CII, namely

- *critical infrastructure object security,*
- *critical infrastructure object owner and/or manager,*
- *vitally important services and functions,*

[50] https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#Text

- *critical information infrastructure objects protection,*
- *critical information infrastructure object identification,*
- *critical information infrastructure,*
- *critical infrastructure sector (subsector),*
- *authority responsible for the sector (subsector), and*
- *restoration time.*

The document contains the description of the steps to be accomplished by responsible authorities for drawing up the relevant lists including, inter alia, CII objects identification and criticality assessment, objects categorization by their criticality. The document establishes the distribution of responsibilities for sectoral (subsectoral) and national lists drawing up and maintenance. According to the Procedure under consideration it is the Administration of the SSSCIPU that is responsible for the national *List of the critical information infrastructure objects* drawing up and maintenance. Owners (managers) of the CII object assigned to the national List of CII objects have primary responsibilities for ensuring protection of such objects against cyberattacks. Information relating to the CII objects included in the national and sectoral lists is defined as that with limited access.

Besides, the form "*Data on critical information infrastructure object to be included in the sectoral/national List of the critical information infrastructure*" is annexed to the *"The procedure for drawing up the List of the critical information infrastructure objects".*

The second annex to Resolution 943 (9 October, 2020) of the Cabinet of Ministers of Ukraine is *"The procedure for the inclusion of critical information infrastructure objects in the State register of critical information infrastructure objects, its drawing up and operation".* The main purpose of the document is to ensure operation of the *State register* designed for keeping records on CII objects of the critical infrastructure objects assigned to categories I and II depending on their criticality. This document includes definitions of the same terms as in the first annex to the Resolution 943 and defines *the register as an information and telecommunication system designed to process and store information on CII objects of the critical infrastructure (CI) objects of categories I and II by their criticality.* The procedure charges the Administration of the SSSCIPU with responsibilities of a register manager and describes in detail the relevant functions.The document outlines information to be submitted to the register, identifies entities responsible for its submission and establishes the time frame and conditions for this action. Access to information stored in the register shall be limited, and the document determines the terms for having it.

Annex 2

The summarty of Resolution №1109 of the Cabinet of Ministers of Ukraine
"On certain issues of the critical information infrastructure"[51]
adopted on October 9, 2020, Kyiv

The resolution has been adopted by the Government in pursuance of Article 6. *The critical infrastructure objects* of the Law of Ukraine "*On basic principles of ensuring cybersecurity of Ukraine*" on October 9, 2020. The document was submitted to the Cabinet of Ministers by the State Service of Special Communications and Information Protection of Ukraine (SSSCIPU).

In accordance with paragraph 1 of resolution the following regulations have been enacted:

1. *Procedure for assigning objects to the critical infrastructure objects;*
2. *List of State critical infrastructure sectors (subsectors) and services provided by them*
3. *Methodology for critical infrastructure objects categorization.*

The purpose of the first annex to Resolution 1009 is to outline the steps needed to assign an infrastructure object to the critical infrastructure. The document contains the definitions of the terms related with critical infrastructure and its protection. Paragraph 2 of the document introduces 12 terms of which five are the same as in Resolution 943:

- *critical infrastructure object security,*
- *critical infrastructure object owner and/or manager,*
- *vitally important services and functions,*
- *critical infrastructure sector (subsector),*
- *authority responsible for the sector (subsector).*

Yet, three of the terms are similar to those in Resolution 943 but addressing *critical infrastructure* instead *critical information infrastructure:*

- *critical infrastructure objects protection,*
- *critical infrastructure object identification,*
- *critical infrastructure.*

Finally, the rest four terms are new ones:

- *critical infrastructure objects categorization,*
- *critical infrastructure object category,*
- *crisis situation,*
- *restoration time.*

Paragraph 3 of the document establishes four criticality categories depending on potential consequences caused by object operation failure from nationwide ones (category I) to those of local level (category IV).

Paragraphs 4 through 8 describe the steps needed to draw up the national and sectoral lists of the critical infrastructure objects including objects categorization

[51] https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text

according to the relevant methodology attached, outlines distribution of responsibilities of the authorized bodies, terms and conditions of list updates and set up the requirement to provide the limited access to information to be protected according to national legislation in the field of information protection.

The second annex to Resolution 1009 is *The List of State critical infrastructure sectors (subsectors) and services provided by them*. The document includes authorities entrusted with responsibilities for the relevant sectors (subsectors) providing critical services. These authorities are the following:

1. Ministry of Energy of Ukraine (fuel and energy sector);
2. Ministry of Digital Transformation of Ukraine (IT-sector);
3. Ministry for Communities and Territories Development of Ukraine (life-support systems);
4. Ministry of Economic Development, Trade and Agriculture of Ukraine (food industry and agricultural sector);
5. Ministry of Health of Ukraine (health care sector);
6. National Health Service of Ukraine (health care sector);
7. National Commission on Securities and Stock Market (financial sector);
8. Ministry of Infrastructure of Ukraine (transport and postal services)
9. Ministry for Strategic Industries of Ukraine (industry);
10. Ministry of Internal Affairs of Ukraine (civil protection of the population and territories).

The CI sectors, where applicable, are divided into relevant subsectors.

The third annex to Resolution 1009 is the *Methodology for critical infrastructure objects categorization* which establishes the procedure and the criteria for assigning infrastructure objects to one of the categories of criticality. Paragraph 2 of the Methodology repeats the definition of terms contained in Annex 1 to Resolution 1009. According to Paragraph 3, a criticality category is determined basing on the analysis of the negative impacts caused by infrastructure object operation failure deriving from criteria presented in attachments 1 and 2 to this Methodology. *Attachment 1 sets up the sectoral criteria* to determine the level of a negative impact on providing basic services in case of object destruction/ damage or CI object operation disruption, *while Attachment 2 — intersectoral ones.* Paragraph 4 presents step-by-step description of object criticaliy determination. When so doing, the level of a negative impact is determined taking into account the social, public and economical significance of a CI object, its interconnections with other CI elements and importance in terms of national security and defense. The attachments to the Methodology include the forms to be completed as well as the mathematical formula to calculate the criticality level of a CI object. Depending on a result of calculations a CI object is assigned either to one of four criticality categories (I, II, III, IV) or is recognized as non-critical one. The methodological recommendations for infrastructure objects categorization are subject to approval by the Administration of the SSSCIPU.