NATIONAL INSTITUTE FOR STRATEGIC STUDIES

DEVELOPING THE CRITICAL INFRASTRUCTURE PROTECTION SYSTEM IN UKRAINE

Monograph

Kyiv 2017

UDC 354+321+355+327
D 94

Published by the decision of Academic council of the NISS
(protocol № 07 of 31 October 2017)
Electronic version: http://www.niss.gov.ua

Authors:

Sergiy Kondratov (Chapters: 1.1; 1.3; 2.1; 2.3; 3.1; 3.2);
Dmytro Bobro, PhD (Chapters: 1.3; 2.3; 3.2; 3.3);
Volodymyr Horbulin, D. Sc., Professor, Academician of the National Academy of Sciences of Ukraine (Foreword; Chapters: 1.3; 2.3; 3.2);
Oleksandr Sukhodolia, D. Sc., Professor (Chapters: 1.1; 1.3; 2.2–2.4; 3.2);
Serhii Ivaniuta, D. Sc. (Chapters: 1.3; 2.3; 3.2; 3.5);
Oleh Nasvit (Chapters: 1.1; 1.3);
Dmytro Biriukov, PhD (Chapter 1.1);
Genadiy Riabtsev, D. Sc., Professor (Chapter 3.4);
General editor: *O. Sukhodolia, D. Sc., Professor*

Reviewers:

Dmytro Dubov, D.Sc. in Political Science, Head of the Department of Information Security and Development of the Information Society National Institute for Strategic Studies;
Oleksandr Lytvynenko, D.Sc. in Political Science, Deputy Deputy to the Secretary of the National Security and Defense Council of Ukraine;
Anatoliy Marushchak, D.Sc. in Law, Director of the Educational-Scientific Institute of Postgraduate Training of the Security Service of Ukraine

D 94 **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.

ISBN 978-966-554-284-1

This publication presents a multiyear work of experts and scholars from the National Institute for Strategic Studies (Energy Security and Technogenic Safety field of research) on implementing in Ukraine the best world policies and practices in the field of critical infrastructure protection.

The publication summarizes these efforts and presents legislative and conceptual documents, analytical and review articles addressing the issues of introduction of the critical infrastructure protection concept in Ukraine. It is the first collection in English showing both the status of progress achieved and problems to be resolved by Ukraine to ensure the level of critical infrastructure protection and resilience adequate to contemporary challenges and threats.

The publication is intended for foreign partners cooperating with Ukraine in the fields of national security, critical infrastructure protection, crisis management, etc. It also will be of use for representatives of Ukrainian public authorities, law enforcement and intelligence agencies, state and private companies, scholars, experts and all of those who interested in the topic of critical infrastructure protection and resilience and related issues.

UDC 354+321+355+327

ISBN 978-966-554-284-1

CONTENTS

NOTATIONS, SYMBOLS, UNITS, ACRONYMS AND DEFINITIONS

AFU	–	Armed Forces of Ukraine
CEI	–	Critical Energy Infrastructure
CI	–	Critical Infrastructure
CMU	–	The Cabinet of Ministries of Ukraine
CS	–	Crisis Situation
CTC	–	Counter-Terrorism Center (at the Security Service of Ukraine)
DBT	–	Design Basis Threat
EU	–	European Union
GP	–	Green Paper on Critical Infrastructure Protection in Ukraine
ICC		Information and Crisis Center (of the State Nuclear Regulatory Inspectorate of Ukraine)
IEI	–	Information Exchange and Interaction
IMOH	–	The Inter-Ministerial Operative Headquarter
MIA	–	The Ministry of Internal Affairs of Ukraine
MoD	–	The Ministry of Defense of Ukraine
MoECI	–	The Ministry of Energy and Coal Industry of Ukraine
MoH	–	The Ministry of Health of Ukraine
MSCU	–	Main Situation Center of Ukraine of the National Security and Defense Council
NCCCS	–	National Coordination Center for Cyber Security of the National Security and Defense Council
NCSS	–	National Cyber Security System
NCCM&CIP	–	National Center for Crisis Management and Critical Infrastructure Protection
NCIPP	–	National Critical Infrastructure Protection Plan
NISS	–	The National Institute for Strategic Studies
NS&CCN	–	National Situation and Crisis Center Network
NSDCU	–	National Security and Defense Council of Ukraine
PHF	–	Potentially Hazardous Facility
PPP	–	Public-Private Partnership
RAW	–	Radioactive waste
RM	–	Radioactive material

SBGS	–	State Border Guard Service of Ukraine
SCCP	–	State Center for Cyber Protection and Cyber Threat Suppression (of the State Service of Special Communications and Information Protection of Ukraine)
SCC	–	Situation-crisis Center
SCN	–	Situation Centers Network
SSCC	–	Sectoral Situation and Crisis Center
SEMC	–	State Emergency Management Center at the State Emergency Service of Ukraine
SESU	–	State Emergency Service of Ukraine
SNRIU	–	The State Nuclear Regulatory Inspectorate of Ukraine
SPPS	–	State Physical Protection System
SRIP	–	State Response and Interaction Plan in the Event of Sabotage against Nuclear Facilities and Nuclear Material
SSSCIP	–	State Service of Special Communications and Information Protection of Ukraine
SSU	–	Security Service of Ukraine
TTX	–	Table-Top Exercise
USSCP	–	The Unified State System for Civil Protection
USSPRM-T	–	The Unified State System for prevention of responding to and suppressing terrorist acts and mitigation their consequences

FOREWORD

State's capacity to confront internal and external threats and to respond adequately to challenges depends on a number of factors to which the developed states assign, inter alia, the levels of critical infrastructure (CI) protection and resilience. And it is understandable, since the main criterion for including objects, systems and resources (whether the listed ones are physical or virtual) in CI is its heavy impact on providing the people, society and State with vital services and unimpeded access to critical resources.

Destruction, breakdowns of such objects and systems, failures and essential limitations in providing vital services and access to critical resources cause rapid-onset impacts for health and well-being of public, sustainable and successful society and national economy functioning, threaten national security and the existence of a State.

Obviously, not all CI objects meet this criterion – some of them have only a limited impact on providing vital services and functions, while the lack of services and products of others may be compensated, at least for a certain period of time, by special measures undertaken. Besides, it is crucial to highlight that the procedure of assigning objects to CI are directly connecting with the state of the national economy, because allocation of funds and other resources for CI protection and resilience depends strongly on State's economic situation. To strike necessary balance between requirements for critical infrastructure protection and resilience, on the one hand, and costs for relevant measures to be undertaken, on the other hand, is a complex task to address which the public-private partnership is to be established, numerous managers, experts, researchers, etc. are to be involved.

One more peculiarity of measures aiming at providing a due level of critical infrastructure protection and resilience is that all of them have

to be developed, approved and tested in terms their efficiency and feasibility taking into account all types of threats (i. e. natural, man-made, criminal and terrorist threats) and their possible combinations. Preparedness to withstand such threats and their combinations raises acutely the issues of coordination, interaction and information exchange among all stakeholders, requires implementation modern approaches to crisis management that seems impossible in Ukraine without charging a special authority with the coordinating function in the field of critical infrastructure protection.

The process of formation of modern approaches to CIP was triggered (like a lot of others in the realm of security) by 9/11. Unfortunately, our country did not pay due attention to this issue for a long period of time, and at the present, one could see Ukraine far behind not only such nations as the U.S., U.K. and Germany, but also, our neighbors – Poland and Czech Republic.

Actually, in Ukraine work in this direction began only several years ago, and the start was made in our organization – the National Institute for Strategic Studies (hereinafter NISS). Several studies on this topic were carried out by the NISS's scholars and their results were presented in a number of publications.

This work entered its active phase in 2013 when NATO Programme for Professional Development in Ukraine agreed to support the NISS in this field. The joint efforts were resulted in development in 2015 and publication in 2016 the *Green Paper on Critical Infrastructure Protection in Ukraine* and some other papers on the subject matter. Due contributions to this publication were made by the Ukrainian experts and experts representing a number of NATO member-states created a solid base for further development of Critical Infrastructure Protection Concept. Later on, close cooperation between the NISS and NATO Energy Security Center of Excellence resulted in organization of the first national level table-top exercise on critical energy infrastructure protection in Ukraine with wide involvement of experts from NATO member-states.

One of the most important outcomes of cooperation with NATO was that with the assistance of NATO experts the «critical mass» of the Ukrainian public servants, scholars, experts, etc. was created, facilitating that the issue was brought to the highest political level in Ukraine. Besides, the hybrid aggression of Russia against Ukraine and damage of

Ukrainian infrastructure also has played its important role in getting awareness on the CI protection and resilience importance[1].

As a result, the breakthrough events occurred early 2017, I mean Presidential Decrees № 8/2017 and No. 37/2017 of Jan 16, 2017 and Feb 16, 2017, respectively, which enacted relevant decisions of the National Security and Defense Council of Ukraine including, inter alia, those aimed at «providing comprehensive improvement of the legislative basis for critical infrastructure protection and creation of a state system to manage its security» and envisaged drafting (with NISS participation) the concept for the creation of the state critical infrastructure protection system after approval of which the draft law of Ukraine «On Critical Infrastructure and Its Protection» should be developed and submitted to Verkhovna Rada (Ukrainian Parliament).

As mentioned before, the important role in the progress achieved in this particular direction, have been played by the experts representing the NATO member-states. Unfortunately, as it was revealed by practical work of the NISS with NATO institutions, the utilization of full potential of international cooperation in the field was restricted by the lack of publications in English presenting results of Ukrainian scholars' studies, methodological tools, conceptual documents, etc. It was decided at the NISS to do all that was in our power to reduce this information gap and to publish the English version of the collection of papers and other materials on CI protection and resilience written and translated by our scholars.

I hope that this collection will be of use for further development of international cooperation of Ukraine, in general, and the NISS, in particular, and for better understanding by foreign experts of the processes, problems and challenges facing Ukraine on its way to protect adequately its CI.

Volodymyr Horbulin,
Director of the National Institute for Strategic Studies,
Academician of the National Academy of Sciences of Ukraine

[1] The World Hybrid War: Ukrainian Forefront: monograph abridged and translated from Ukrainian / Volodymyr Horbulin. – Kharkiv: Folio, 2017. – 158 p. Retried from http://www.niss.gov.ua/public/File/book_2017/GW_engl_site.pdf

PART I
ESTABLISHING THE CRITICAL INFRASTRUCTURE PROTECTION SYSTEM IN UKRAINE

1.1. THE GREEN PAPER ON CRITICAL INFRASTRUCTURE PROTECTION IN UKRAINE[2]

INTRODUCTION

The Ukrainian state currently faces the most serious security challenge in its entire independence period. Acute social and political crisis against the backdrop of foreign military involvement in the internal affairs of Ukraine, abrupt surge of extremism and terrorism, unseen growth of crime, including armed, decline of economy and expanding humanitarian crisis in the eastern regions of the country, destruction or damage of numerous enterprises and infrastructure objects are the factors that define the new reality in which Ukraine currently exists and in which security of its citizens, the society and state institutions should be assured.

Quite obviously, the Ukrainian security sector is in need of a radical reform that should account for international experience and the declared course toward integration in the EU. In the current environment, the factors described above make implementation of the critical infrastructure concept, actively used in leading Western countries, the EU and NATO member states as one of the security policy tools, particularly topical.

The definition of CI generally covers such objects, systems, networks or parts thereof whose disruption or destruction will cause severe consequences for the state's social and economic sectors, affect its defense potential and national security. Furthermore, the functioning of CI at the time of peace is associated with the sustaining of vital functions of

[2] The Green Paper was published in October 2015.

the society, protection of basic needs of its members and giving them a feeling of safety and security.

As well as any other country, Ukraine has such systems, objects and resources whose destruction or damage will have major adverse effect on citizens, the society and government institutions. It would be a mistake to say that in our country no attention is paid to their protection and security. On the contrary: there is a range of laws and regulations that define authority and competence of government agencies in this sector and associated sectors, set the requirements for protection and assurance of secure operation of such objects and systems. Nonetheless, Ukraine still lacks a nation-wide systematic approach to management of protection and security of the whole aggregate of such systems, objects and resources, considering mutual interface between some objects customarily attributed to critical infrastructure. Furthermore, there is still no mechanism to prevent potential crisis situations associated with CI operation.

Implementation of such a mechanism would require profound survey of existing practice for critical infrastructure protection (CIP) in Ukraine, currently dominated by departmental approaches, as well as analysis of interaction and coordination between appropriate government agencies, ways and practices of business involvement in the enhancement of security and resilience of critical infrastructure.

This Green Paper has been developed to support nation-wide expert discussion of key problems in establishment of a critical infrastructure protection system for Ukraine and ways to address them, which will be a valuable input in the process of systematic reform of the entire national security sector making its structure and functions closer to those existing in the EU and NATO member states.

WHAT CRITICAL INFRASTRUCTURE MEANS

For stable and safe existence, a contemporary society and its members should sustainably receive a number of various products and services, should have access to a number of critical resources, etc. For this purpose, a number of assets, networks and systems, both physical and virtual, should be created and operated.

Rapid development of technologies, particularly in the IT sector, observed in the past decades, caused dramatic – sometimes even

revolutionary – changes resulting in the increased interrelation, inter-penetration and interdependence of varied networks and systems, production, finance, commerce and other processes in all spheres of life of most countries worldwide. This substantially increases vulnerability of such systems and objects and much complicates assurance of their reliable protection and security. These processes unfold against the backdrop of abrupt escalation of terrorist threats, particularly at the international scale, an increase number of man-induced disasters, including those caused by human factor, a larger number of natural disasters caused, inter alia, by global climate change. All these factors explain the level of attention paid by the leading countries to protection of objects, systems and resources most critical for security of their citizens, societies, and states.

Definition of Critical Infrastructure

Considering a large number of factors that one way or the other influence life of contemporary people, societies or states, it is imperative to clearly define the scope of those systems, networks and objects whose operation supports services and functions critically important for the existence of the public, the society and the state. This is the question to which the definition of «critical infrastructure» should answer.

Note that, albeit similarity of definitions given in legislations of leading nations and international organizations, there are differences that, obviously, reflect national or institutional (in case of the EU or NATO) application of this term in their regulatory systems.

The laws of the USA, being the leader in the developing this security area, interpret CI as *«systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health and safety, or any combination of those matters».* (USA Patriot Act, 2001).

In Germany, CI includes *«institutional and physical structures and objects so vital for the society and economy of the state that their failure or deterioration will result in sustainable disruption of supply, substantially undermine state security or cause other dramatic consequences».*

The United Kingdom has defined the following CI elements: *«such installations, systems, assets and networks necessary for the functioning*

of the state and provision of vital services, on whom everyday life in the United Kingdom depends.» In the Netherlands definition of CI includes *«products, services and associated processes».* There are also other examples of different definitions given in national laws.

In our opinion, the important part is in that in some national legislations the accent is somewhat shifted from the physical dimension, that is, vital systems, assets and resources, toward their functions and services already in the definition of CI. It is functions and services provided to the society, business and the state by CI assets and systems that are used as the basis for the definition of their criticality, which provides effective methodology for setting CI element selection criteria and protection priorities[3].

Obviously, definition of this key term in the Ukrainian legislation, while remaining within the framework of accepted international approaches, should fully reflect the security environment in Ukraine.

The term «critical infrastructure» has been used in Ukrainian regulations on numerous occasions, however there is still no definition in applicable laws. The first reference to critical infrastructure in an official document occurred in 2006 in the text of the Recommendations of Parliamentary Hearings on the Development of Information Society – alas, with no subsequent development. In the National Security Strategy «Ukraine in the Changing World» (2012), this term was mentioned in the context of defining ways to enhance energy security an avenues to assure information security.

The new National Security Strategy for Ukraine (2015) gives more detail to the CI definition. For the first time it singles out threats to CI among «current national security threats»; furthermore, the section on threats to cyber security and information resources mentions vulnerability of critical security objects to cyber-attacks. Besides, critical infrastructure security has been mentioned for the first time as one of the «key areas of the state policy for national security», and its priorities have been identified.

[3] For instance, energy sector is attributed to critical infrastructure by all countries, as well as by such international associations as the EU and NATO. Main function (service) of this sector is to cover energy demand of the population, society and the state. With accent placed on energy assets and systems, this, failing proper analysis, could result in priority given to power generation facilities, although power supply assets are more important to provide power supply services to the end consumer. As seen from the international experience, the severest from the standpoint of power availability to the society have been the consequences of accidents in electricity transmission and distribution systems, rather than in case one or more generating facilities failed.

Absence of CI definition in the Ukrainian legislation and, consequently, absence of a list of assets that could be attributed to such infrastructure have on numerous occasions blocked high-priority security tasks, such as in paragraph 6 of the Resolution of the National Security and Defense Council of 1 March 2014 *On Immediate Measures to Assure National Security, Sovereignty and Territorial Integrity of Ukraine* (enacted by the Presidential Decree No. 189/2014 of 02 March 2014), whereby the Ministry of Internal Affairs of Ukraine is ordered to assure «enhanced security of energy sector and critical infrastructure assets».

Considering the above and referring to the experience of leading nations in development of approaches to assuring national security through application of the CI concept we suggest the following definition of this term for Ukraine:

> *Critical infrastructure of Ukraine* shall mean and include systems and resources, whether physical or virtual, that support functions and services whose disruption will cause most severe negative effects for activity of the society, socioeconomic development of the country and national security.

This definition does not emphasize interrelation/interdependence between individual CI elements; however, this is believed to be important from the consequence level perspective. In other words, security management of individual assets should be based on appreciation of the system-wide functions of the entire CI.

Another term to be defined is «critical infrastructure protection»:

> *Critical infrastructure protection in Ukraine* shall mean and include a set of measures implemented in regulatory, institutional and technology tools directed toward assurance of critical infrastructure safety, security and resilience.

Critical infrastructure resilience will be understood as its capability of reliably operating in the normal mode, adapt to continuously changing environment, withstand and quickly recover from accidents and technical failures, malicious acts, natural calamities and hazardous natural

phenomena[4]. Note also that «safety and security» as used in the definition of critical infrastructure protection covers both security per se (including physical protection), operational security, and safety.

Sectors, Assets, Systems and Resources Attributable to Critical Infrastructure

Lists of sectors attributed to CI in various countries are also largely similar, considering uniformity of trends that shape the development of current society. Existing differences are primarily caused by national conditions, tradition and nature of security policy of the given state or international organization.

Referring to the US experience in the area we will note that the list of sectors considered to form national CI of this country is, probably, the most comprehensive and includes 16 items:

- Chemical;
- Commercial facilities;
- Communications;
- Critical manufacturing;
- Dams;
- Defense industrial base;
- Emergency services;
- Energy;
- Banking and finance;
- Food and agriculture;
- Government facilities;
- Healthcare and public health;
- Information technology;
- Nuclear reactors, materials and waste;
- Transportation systems;
- Water and wastewater systems.

In Germany, CI is divided into two groups including altogether nine sectors: *vital (absolutely necessary) base technical infrastructure* (energy supply, information and communication technology, transport, water

[4] This interpretation is in line with the definition of resilience used in formal documents of both the European Commission and a number of developed states, as well as in the US President Directive № 21 (February 2013).

supply and household waste removal) and *vital (absolutely necessary) socioeconomic service infrastructure* (health care, food supply; emergency services, rescue services, incident control services; parliament, government, government executive bodies, law enforcements; finance sector and insurance companies; mass media and culture heritage assets). It is noted that a strong interrelation exists between these groups since practically all socioeconomic services largely rely on unrestricted access to base technical infrastructure, whereas base technical infrastructure, in its turn, depends on availability of socioeconomic services, such as a permanent legal service or first aid and emergency response services.

Obviously, Ukraine, struggling amid stringent security, financial and economic conditions, should compile its CI sector list proceeding primarily from available resources and the need to sustain and protect base functions, failing which safe existence of the population, the society and the state as well as due protection of national interests will be compromised.

A tentative list of Ukraine's CI sectors is provided in Annex A. The next step following identification of CI sectors should be to list individual CI assets, systems and resources (elements). This list should be anywhere from several dozen items for smaller countries to many thousands (e.g., in case of the US). Since each country has only limited resources that could be allocated for the national infrastructure protection, national laws should set criteria by which certain assets or systems are attributed to CI, based on approved methods to assess threats and risks for its sustainable operation. Such lists are used for the planning of appropriate measures, as well as in the decision making process. They are typically subject to revision – either periodically or in case of dramatic changes in the security environment or major amendments to the national legislation, etc.

Based on the above we suggest considering the definition of criticality provided in the German National Critical Infrastructure Protection Strategy: *criticality is a relative measure of importance of given infrastructure that accounts for effects of its abrupt breakdown or functional failure for security of supply, i. e. for provision of the society with critical goods and services.*

Analysis of existing approaches to identification of CI elements (attribution of assets to critical infrastructure) proves that characteristics to be taken into account may include as follows:

- scale (geographical span of the territory that will be significantly affected by loss of a critical infrastructure element);
- interrelation between critical infrastructure elements;
- duration of effect (how exactly and when damage, caused by the loss, failure, breakage or functional disruption of a critical infrastructure object, will manifest);
- assets vulnerability to hazardous factors;
- severity of potential consequences in the following areas:
  - economic safety (impact on GDP, direct and indirect economic losses, market share of the product, number of personnel employed, tax revenue);
  - life and health safety of the public (number of the victims, dead or seriously injured, number of evacuated population, performance of emergency response services, emergency assistance to the public);
  - domestic and national security (loss of assurance of government's capabilities, loss of authority by the government, disruption of public administration);
  - defense potential (combat degradation of armed forces, disclosure of secret information);
  - environmental safety (impact on natural environment).

Level of detail in describing consequences depends on the CI sector.

CI elements identification should include analysis of interfaces between such elements and evaluated consequences of their potential failure (accident, etc.) in the long run.

Asset Categories in the Ukrainian Legal Framework Approaching the Critical Infrastructure Concept

The Ukrainian legislation concerning protection of assets that, based on the international practice, are attributed to CI, is rather diverse and includes numerous regulations, mostly at the departmental scale.

Applicable legislation provides for the following categories of assets subject to special protection and operation regimes:

- enterprises of strategic significance for economy and national security [1];
- vital assets in energy sector [2];
- vital assets in oil and gas sector [3];

- important governmental facilities, including control centers of government agencies and local government bodies [4];
- potential terrorist targets [5];
- assets to be protected and defended in emergency and during special periods [6];
- assets subject to mandatory protection by State Protection Service on a contractual basis [7];
- high hazard facilities [8] (including from the List of Extremely Hazardous Enterprises Whose Operation Requires Special Arrangements for the Prevention of Detriment to Human Life and Health and to Property, Installations, and the Environment [9]);
- assets included in the State Register of Potentially Hazardous Facilities [10];
- radiological hazard facilities subject to development of a facility-level design basis threat (DBT) [11];
- assets assigned civil protection categories [12];
- assets owned by business entities, whose design should account for requirements of engineered civil protection facilities [13];
- emergency service operator – service 112 (free phone number) [14];
- emergency rescue services;
- National Confidential Communication System [15];
- payment systems [16];
- culture heritage sites [17].

Some of the above categories may be fully or partly attributed to CI, based on the appropriate analysis.

MAIN THREATS TO CRITICAL INFRASTRUCTURE

Leading nations who declared protection of CI and enhancement of its resilience to be high-priority security tasks in the aftermath of the 9/11 terrorist attacks believe it should be protected against all threats (*all hazards approach*).

As a rule, national legislations of the leading nations distinguish between three main categories of threats to critical infrastructure, based on their origin. Yet, even here there are differences. Say, in the US and Canada the range of threats to CI includes *malicious acts* (malicious acts of groups or individuals, such as terrorists or criminals),

natural hazards (hurricanes, tornadoes, earthquakes, tsunamis, floods, extreme weather conditions etc.) and *man-induced emergencies* (air crashes, nuclear accidents, fires, power supply system accidents, releases of hazardous substances etc.) In Germany, there are threat categories as follows: *hazardous natural phenomena* (extreme weather conditions, forest and steppe fires, seismic events, epidemics and pandemics, cosmic phenomena); *technical accidents/human errors* (system failures, accidents and emergencies, negligence, administrative errors etc.); *terrorism, crime, war* (terrorism, sabotage, crime, civil wars, hostilities).

Threats under each of the above categories, should they materialize, may cause such negative effects that, in their turn, will become initiating events for threats in other categories and at other CI elements. In this event we speak about the so-called domino effect and/or cascade effect.

As for the spectrum of CI threats existing in Ukraine, their nature is shaped by the security environment currently faced by the country. Hostilities as part of the Anti-Terrorist Operation in Donbas Region, featuring high level of wear of capital assets and serious problems with environmental and anthropogenic safety, rapidly increases the level of threat of accidents at high hazard assets such as coal mines, power sector facilities, chemical factories and steelworks, as well as in the utility networks, whether as the result of incidental damage or loss of process control or as a consequence of terrorist acts or sabotage.

Note that this Green Paper for Critical Infrastructure Protection in Ukraine does not focus on critical infrastructure protection (CIP) in the context of hostilities or during law martial, which should be a subject of other documents.

No doubt, developments in the Eastern Ukraine will have significant impact on threats to the national CI. In particular, it should be expected that a high level of terrorist, sabotage and criminal threats to CI is likely to persist in a long run as the result of today's crisis.

The existing Ukrainian legal framework governing issues allied to CIP classifies emergencies, rather than threats, inter alia based on their origin. Article 5 of the Civil Protection Code of Ukraine specifies that, depending on origin of events that may cause emergency situations in Ukraine, the following types of emergency situations could be distinguished: 1) man-induced; 2) natural; 3) social; 4) military. In our view,

this classification cannot be adopted straightforwardly for the classification of CI threats since it has some methodology reservations and blocks some of the advantages offered by implementation of the CIP concept.

It makes more sense to define the following classes of threats for the purposes of CI:

- *accidents and technical failures,* including air crashes, nuclear accidents, fires, power supply system accidents, releases of hazardous substances etc., system failures, accidents and emergencies caused by negligence, administrative errors etc.;
- *hazardous natural phenomena,* including extreme weather conditions, forest, steppe and peat-bog fires, seismic events, epidemics and pandemics, cosmic phenomena, hurricanes, tornadoes, earthquakes, tsunamis, floods, etc.;
- *malicious acts,* including malicious acts of groups or individuals, such as terrorists or criminals, as well as hostilities under conditions of war.

The highest is the hazard from combined threats and threats whose materialization may cause disastrous and varied cascade effects as the result of interdependence of CI elements.

Accidents and Technical Failures

Looking into *accidents and technical failures* it should be noted that the high level of obsolescence of Ukrainian capital assets creates threat of accidents at high hazard facilities, power sector facilities and in utility networks. Significant risk of man-induced accidents is created by a large number of assets classified as potentially hazardous (over 24 thousand across Ukraine), with nearly a quarter identified as extremely hazardous[5]. According to the State Emergency Service of Ukraine (SESU)[6], accidents at 955 facilities on the State Register of Extremely Hazardous Assets may cause national or regional level emergencies that may threaten critical infrastructure, inter alia as concerns the functioning of fuel and energy assets, bridges and roads, municipal infrastructures etc.

[5] National Report on Anthropogenic and Natural Safety in Ukraine in 2014. – Retrieved from www.dsns.gov.ua/files/prognoz/report/2014/ND_2014.pdf

[6] National Report on Anthropogenic and Natural Safety in Ukraine in 2013. – Retrieved from http://www.dsns.gov.ua/files/prognoz/report/2013/%D0%A1%D0%90%D0%99%D0%A2_%D0%94%D0%A1%D0%9D%D0%A1.rar

Natural Disasters and Hazardous Natural Phenomena

Natural Disasters and Hazardous Natural Phenomena may include:

- meteorological or extreme weather conditions (snowfall, sleet, snowstorms, rain showers, hail, ground frost, drought, extremely hot weather, hurricanes, squalls, tornadoes);
- geological conditions (inundations, mudflows, river floods, impoundments, tsunamis);
- seismic events (earthquakes);
- geological events (hazardous exogenic geological processes: landslides, subsidence and caverns);
- solar physical events (geomagnetic solar storms);
- forest, steppe and peat-bog fires;
- epidemics and pandemics, epizootics, epiphytotic.

Out of the above threat types weather related threats deserve special attention due to significant raise of their frequency in Ukraine in the recent decades. These include ice loads, impoundments, draughts etc.

In hydrological threats category river floods should be treated as the most hazardous considering the consequences for critical infrastructure. A major flood that occurred in Ukraine in 2008 caused damage to more than 500 road bridges, 1660 km of roads of various categories, etc.

Hazardous exogenic geological processes (impoundments, subsidence, caverns and landslides) also pose a serious threat for the functioning and security of critical infrastructure. Up to 20 % of railroad tracks are potentially affected by regional land impoundments, another 40 % are located in the caverned areas, and up to 11 % in the areas of potential landslides. Up to 59 % of trunk gas supply lines are in the likely areas of caverned rock and up to 21 % in the regional areas of potential impoundment. Activation of potentially hazardous exogenic geological processes aggravates geotechnical conditions in which industrial installations and engineering utilities of urban and industrial areas have to be operated.

Malicious Acts

Challenging military and political situation in which our state has to fight for its territorial integrity and sovereignty involves substantial increase in *malicious threats*, including terrorism and sabotage targeting CI assets in Ukraine.

By far the most serious is a potential threat of use of nuclear power facilities for terrorist purposes. It should be noted that the level of physical protection presently secured at the Ukrainian NPPs is adequate given current threats.

Dramatic growth in the intensity of cyber-attacks on Ukraine's information and telecommunication infrastructure has been registered. Targets of cyber-attacks via Internet include servers of government agencies, large companies, finance institutions, political parties, mass media and, more recently, information and telecom infrastructure of military facilities.

Security of the functioning of government authorities, armed forces, law enforcements and special services (buildings, associated infrastructure) during crises deserves special attention. In developed nations, such infrastructure assets are typically attributed to CI.

In addition to the classification by origin, threats to CI could be viewed from the perspective of their targets, including:

- *physical elements,* including equipment and resources of critical infrastructure assets;
- *management and communications systems,* including automatic control and regulation systems, communications systems etc.;
- *facility personnel,* including dispatch and operations personnel covering immediate operational needs of critical infrastructure in the real time.

Identification of threat targets offers a more systematic approach to the formation of the state policy and organization of a CIP system. CIP plans developed by operators and approved by appropriate government authorities should detail measures to suppress threats in the following protection areas:

- *physical protection* aimed for assurance of asset security from unauthorized access, prevention and suppression of sabotage, theft or any other unauthorized removal of equipment, devices, or material;
- *technical protection* that includes enhancement of failure resistance and resilience of systems and their functional redundancy;
- *personnel*, including the training and testing of personnel, controlling their ability to perform prescribed functions and personnel security;
- *information technology*, including protection of information, communication and control systems;

- *legal area*, including personnel response and infrastructure operation in crises, regulatory and legal documentation in respect of appropriate responsibilities, development of guides and instructions for personnel, including on coordination in crisis;
- *recovery plans*, including creation of plans, reserves and services for quick recovery of lost functions.

STATE POLICY IN CRITICAL INFRASTRUCTURE PROTECTION

The aim of Critical Infrastructure Protection in Ukraine

Enhancement of security and resilience of the national CI against the entire range of threats and risks is one of the priority aspects of Ukraine's security policy as it is CI that supports services and functions vital for the population, society and state failing which their secure existence, welfare and appropriate level of national security would not be possible.

The goal of CIP in Ukraine is prompted by the CI definition and is to secure supply of vital goods and services to the population, society, business and state. For CI to perform this function it is necessary to warrant uninterrupted and sustainable operation of CI assets in prescribed modes and to be able to prevent destruction or irreparable harm, stoppage or loss of control of CI assets as a consequence of effect of all factors, as well as to assure quick recovery of their operation where it was disrupted.

Strategic Objectives of the State Policy in Critical Infrastructure Protection

CI of a modern state is a highly sophisticated set of diverse elements including a number of organizational structures, various management models, dependent and interdependent functions and systems in both physical and virtual spaces. CI management involves government agencies at all levels and with various authority and areas of responsibility, as well as owners and operators of assets and systems being part of CI. In the global context, national security, production, economy and finance of each country much depend on factors that define state of security in other countries, as well as in the global dimension.

The emerging new security philosophy builds on common efforts of a citizen, society, business, and state. The «risk management culture» is underway to become a basis of critical infrastructure protection policy and to include:

- open exchange of risk related information between state authorities, private sector, the public and individuals, subject to protection of certain (sensitive) information;
- cooperation between all parties to the critical infrastructure protection process in prevention of and response to incidents;
- enhancement of self-protection and self-assistance and of capabilities of organizations and individuals vulnerable to termination or deterioration of services provided by critical infrastructure[7];
- active international cooperation in critical infrastructure protection considering globalization processes and growing dependence of security, economic, production, financial and other processes in many countries on supply of services and resources to be provided by international networks, systems, companies, etc.

The above relates to the first strategic objective of the CIP policy: *development of security partnership to enhance security and assure resilience of the national CI.*

In most countries in the world, as well as in Ukraine given its successful economy reforms, it becomes obvious that CI assets will be mostly privately owned. It is private operators that own most CI assets and that take the lead in developing new production and protection technologies.

Note that in most developed nations main responsibility for security of CI assets/systems is vested in their owners/operators. They are the ones to secure reliability, resilience and sustainability of their assets/systems. The state should provide appropriate information to owners/operators, create an adequate regulatory framework and incentives for investment in CI security and conditions for continuing competitiveness of business making required investments in CI security.

Thus, effective public-private partnership (PPP) becomes a key element of the successful and sustainable policy directed to uphold proper level of critical infrastructure security and resilience. In the US and in

[7] E. g., in Canada population should be prepared to support their own primary necessities in an emergency situation within at least first 72 hours.

Germany establishment of trust relationships[8] between partners and incentives for cooperation is believed to be a prerequisite to such partnership. National policies should stimulate both private owners and executive government authorities at all levels to create such a system to protect vital infrastructure of the society that would be able to overcome emergencies and reduce risks and consequences of such situations. Incentives for investment in CI security and conditions for sustaining competitive power of enterprises duly investing in CI security should be a mandatory element of such partnership.

Thus the PPP mechanism creates the foundation for promotion of investments in CIP through support of adequate awareness of the business sector of threats and risks for CI elements and of understanding that expenses of the business sector for appropriate arrangements should be balanced and should not undermine its competitiveness and capability of providing services critically important for the population, society and state.

As for Ukraine, before 2014 PPP mechanisms were practiced predominantly in the economy within the framework of the Law of Ukraine *On Public-Private Partnership* of 01 July 2010 № 2404-VI whose provisions do not apply to CI protection activity. At the same time, events of 2014 and 2015 have demonstrated the importance of involvement of the public in protection of national interests of Ukraine and, inter alia, in critical infrastructure protection.

Ukraine is in need of proper regulatory governance of the public-private partnership mechanisms in CIP. It also requires development of a legal framework for mutual obligations of the state and non-government subjects in respect of CIP and for implementation of risk analysis and contingency planning practices, as well as mechanisms and tools for coordination between government and non-government subjects and the public and the responsibility sharing mechanisms (including in respect of financial responsibilities) in the activity of business entities.

Note that the activities in enhancement of reliability, resilience and sustainability of assets/systems will require from operators additional

[8] U.S. Department of Homeland Security, National Infrastructure Protection Plan, NIPP 2013. Partnering for Critical Infrastructure Security and Resilience. – Retrieved from //www.dhs.gov/national-infrastructure-protection-plan

expenditure, which may cause elevated costs of products/services provided by appropriate assets/systems. As a consequence, the respective goods/services will have higher market prices. This socioeconomic aspect of CIP should be taken into account both in identification of CI assets and in setting requirements for their protection. Any requirements for CIP enhancement, initiated by the state, should be well thought-over considering the above socioeconomic dimension. In addition, for certain CI sectors the government, represented by appropriate regulators, might consider revising tariffs for goods or services (such as electricity).

Appropriate information exchange is believed to be one of the most important tools to establish trust between public and private partners, both in the U.S. and elsewhere in the developed world.

In this light the second strategic objective of national CI policy is generally formulated as *establishment of information exchange,* including acquisition, analysis and acknowledgement of information concerning threats and risks for CI, vulnerabilities and characteristics of protection systems for CI elements, response mechanisms and procedures, etc.

In the modern world, CI elements have sophisticated vertical and horizontal ties, what enables cascade and delayed/remote negative consequences of a failure of a certain CI element. As it has been mentioned, in most developed states responsibility for CI assets/systems security is vested in their operators. However, management of private companies often have neither proper awareness of the need for critical infrastructure protection, nor motivation to do so, from the standpoint of narrow corporate interests.

Only agencies authorized by the state may have sufficiently complete data and information concerning risks and threats for both the entire CI and its separate elements; they, however, require detailed information and cooperation from the private sector. In this light, establishment of an adequate legal framework for exchange of information on secure functioning of CI or protected systems becomes important. Where this objective is attained, the partners effectively exchange information (including intelligence) on various aspects of CIP (including best practices) based on established procedures and assure protection of sensitive information (including commercial) that may be used for malicious purposes.

The Ukrainian state should duly govern the information exchange issue, inter alia through development of general information exchange standards, regulation of activity of operators' personnel responsible for information exchange, methods of information processing and analysis, communication of potential and real threats to infrastructure operators, and setting requirements and limitations on use of sensitive information to prevent abuses.

In most developed nations strategic objectives also include development of a CIP system and enhancement of its resilience based on the *all-hazard risk management approach.*

Based on the international experience, the first step en route to achieving this objective is identification of all threats and risks for CI of Ukraine, based on their comprehensive analysis. The following risk management arrangements are expedient for the purpose of risk reduction[9]:

- enhancement of CI resilience to identified threats and hazards;
- prevention of threats related to malicious acts (terrorism, criminal activity, etc.);
- planning timely response to failures in CI operation in order to reduce negative impact on public health and safety, economy and basic functions of the state;
- planning quick renovation and recovery of CI functions in case of emergency that cannot be prevented.

Albeit vital importance of CI security and resilience enhancement measures their planning in any country is subject to budgetary and resource limitations. In this view *maximum efficiency in use of resources for critical infrastructure protection* is another strategic policy objective in this area. Developed partnerships at both national and international levels, coordination of activities and information exchange between partners create prerequisites for achieving this objective, which results in elimination of duplicated functions and avoidance of diffusion of resources among individuals CIP subjects.

Considering financial and economic hardships currently faced by Ukraine this objective becomes particularly topical.

Ukraine should ensure establishment of the state-level CI threats and risks assessment system, proper interface between government

[9] U.S. Department of Homeland Security, National Infrastructure Protection Plan, 2006. – Retrieved from http://www.naruc.org/publications/nipp_plan4.pdf

authorities and coordination of activities of various parties involved, which will require appointment and appropriate empowerment of a designated government authority.

Obviously, strategic objectives of Ukraine's state policy in CIP should be reflected in the national legislation. Inter alia, it appears expedient to develop a separate Law of Ukraine; suggestions as to its structure are presented in Annex B.

Main Principles of Critical Infrastructure Protection Policy Formation in Ukraine

Priorities of CIP policy for Ukraine have been formulated based on the significance of CIP for national security of a modern state. Principles which should be in the basement of such protection are of strategic security importance.

In our view, main principles for the formation (development) of CIP policy for Ukraine should include as follows.

Principle of coordination, which means:

- planning security at the national level; coordinated development of regulatory, institutional and scientific tools for the performance of CIP tasks;
- consideration of the need for CI security in planning, prioritizing and assessment of the nation's socioeconomic development;
- establishment of mechanisms to impact CI security state;
- operation of a single center for CI security state assessment, threat forecasting and risk assessment for CI assets and for coordination of efforts of all stakeholders in CIP;
- establishment of mechanisms to coordinate efforts of all stakeholders, including government, business sector, and society, for critical infrastructure protection, including horizontal links between operators of interdependent and homogeneous CI assets;
- control of all resources available to the state for their rational use;
- implementation of a state-level DBT for CI and individual elements thereof based on a national security threat assessment;
- planning of human resource development considering available capabilities of specialist learning institutions.

Principle of methodological unity in CIP, under which the CIP concept should be implemented through:

- use of a uniform conceptual and methodology framework to analyze CI threats;
- development of a methodology to identify (list) CI assets based on assessment of importance of goods/services they provide (criticality assessment);
- consideration and assessment of the entire scope of threats for CI assets; use of risk-oriented methods for risks and threats analysis and forecast;
- periodical assessment of threats, risks for and vulnerabilities of CI assets on the basis of appropriate experience;
- identification of CIP requirements in the time of peace (both on a day-to-day basis and in a critical situation or in national emergency), as well as during a special period (considering specific conditions during the mobilization period, law martial, and recovery period);
- equal attention to prevention of emergency threats, enhancement of preparedness to response to and elimination of consequences of emergencies;
- combination of physical protection and measures to secure reliability, resilience and capability of quick recovery;
- assurance of defense in depth and diversity of protection barriers;
- gradual implementation of regulatory, institutional and scientific tools for enhancement of means and measures for CIP.

Public-private partnership principle means involvement of all stakeholders in CI operation and sharing responsibilities among them (state/owner; government/society; regulator/operator).

Implementation of this principle should cover:

- exchange of risk related information between government agencies, the private sector, the public and individual citizens, subject to appropriate protection of certain (sensitive) information;
- use of resources of both the state and the private sector to attain CIP objectives;
- declaration of asset security by its owner/operator;
- certification of CI assets;
- partnership sharing and allocation of responsibilities for security, safety and resilience of critical infrastructure between the operator and the state;
- creation of incentives for investment in critical infrastructure security; making provisions for competitiveness of businesses making due investments in CI assets/systems security;

- involvement of the public and expert community, use of consultative committees to identify requirements for CI security, safety and resilience.

Confidentiality principle means that sensitive information concerning vulnerabilities and specific characteristics of facility protection systems, as well as commercial information should not be disclosed, save in the events prescribed by applicable laws, since it may be used for malicious purposes.

International cooperation principle means consideration of transboundary effects of CI operation, international obligations of Ukraine concerning operation and security of CI and involvement of Ukraine in European civil protection, cyber security and terrorism suppression mechanisms.

CRITICAL INFRASTRUCTURE PROTECTION SYSTEM OF UKRAINE

Key Tasks of Critical Infrastructure Protection System of Ukraine

Based on the objectives and principles of a CIP system the following *key tasks* of this system could be formulated.

a) *General coordination of CIP in Ukraine,* which inter alia includes:

- creation and support of a national center for crisis management and CIP;
- formulation of proposals for improvement of legal framework for national security and defense (specifically as concerns civil protection, suppression of terrorism and cyber-threats) related to CIP;
- assessment of threats for CI at the national level with consideration for interrelations between individual infrastructure assets and sectors, impact of all types of threats, and assessment of risks at regional and national levels;
- decision on and notification of change of A CIP system operation mode depending on a threat level, change of legal status (time of peace, state of emergency, special period);
- preparation of a national critical infrastructure protection plan (NCIPP);
- preparation of a state-level DBT for CI;
- coordination of efforts of all stakeholders (government agencies, local governing bodies, business sector and society) regarding critical

infrastructure protection, including horizontal interface between operators of interdependent and homogeneous critical assets;

- coordination and information exchange with the network of security and defense crisis (information analysis) centers;
- preparation of a government target program for critical infrastructure protection;
- formulation of a comprehensive research and development program for critical infrastructure protection;
- coordination (assignment of a point of contact) with EU structures and government authorities of EU member states.

b) *Prevention of crisis situations, preparedness to actions in crises, governance in emergency situations related to CI (CI assets), recovery of critical infrastructure functions,* including:

- application of existing and establishment of new measured for prevention of potential crises related to operation of CI (or individual sectors or assets thereof);
- CI preparedness and ability to function amid crisis;
- creation of new and improvement of existing tools (regulatory, institutional and technological) for prevention of and governance in crises related to CI (or individual sectors or assets thereof);
- preparation, within the framework of the NCIPP, of the plans to prevent crises related to critical infrastructure;
- physical protection of CI assets, prevention of unauthorized acts (including acts of terrorism) against CI assets, mitigation of negative consequences for and recovery of CI assets where unauthorized acts have occurred;
- protection of CI infrastructure assets against cyber-attacks, protection of data and technical information in process control systems at critical infrastructure facilities against unauthorized locking or modification;
- assurance of the requisite level of operational safety at CI assets, development and implementation of engineered security measures for CI;
- assurance of stable CI operation in emergency situations and during special periods;
- stockpiling materials reserves; assessment and inventory tracking of resources;
- assurance of information confidentiality based on prescribed legal requirements in processing CI asset data;

- recovery of CI operation in the event of an accident/failure, a malicious act that disrupted its operation, or under effects of natural phenomena.

c) *Decision support in CIP,* including:

- monitoring and identification of potential crises related to CI operation;
- formulation of proposals for prevention of CI threats;
- definition and revision of requirements for CIP in various operation modes;
- identification of CI assets; maintaining an automatic CIP register (list); acquisition, collation and analysis of data concerning CI objects and their operation;
- assurance of operation of an information exchange system, continued monitoring, analysis and forecasting of threats for CI assets;
- identification and assessment of interdependence between CI assets;
- identification and forecasting of amounts of resources required for CIP;
- support of decisions concerning response to emergencies related to CI security and resilience;
- efficiency analysis of administrative and technical arrangements to reduce risks for vital activity amid potential and real threats to CI operation.

d) *Application of CIP monitoring and control mechanisms,* including:

- early notification (threat warning) of CI asset operators and information, consultative, expert and technological support for CI operators and service consumers (the public) for the prevention of, response to and mitigation of potential impact of such threats;
- change of A CIP system operation modes depending on threat level and legal status;
- implementation of automatic systems for early detection and notification of emergencies;
- development and implementation of standards, norms and regulations for CIP;
- checks and assessment of CI asset security;
- checks and assessment of information security at CI assets;
- formation, accounting and renewal of CI assets certificates and risk cards for localities.

e) *International cooperation in CIP*:

- assessment of transboundary effects of CI operation and of transboundary threats;
- exchange of information and best practices in CIP;
- Ukraine's involvement in EU mechanisms for critical infrastructure protection;
- analysis of EU (as well as USA and other countries) regulatory requirements and their potential implementation in Ukraine.

Note that some tasks mentioned in the list above are partly covered by existing Ukrainian systems for civil protection, counterterrorism, suppression of cyber-threats, and assurance of national defense capability. However, most tasks are fundamentally new and relate to principles of critical infrastructure protection policy that, in their turn, reflect strategic objectives of the national policy in this area.

Some of the CIP system objective and tasks on the above list deserves special attention. The first group of tasks related to general coordination includes a paragraph on establishment and support of a *national center for crisis management and critical infrastructure protection* (NCCM&CIP). Such institutional novelty should address the task of organizational support for a CIP system. NCCM&CIP that may be established as a separate agency or as a structural unit within a government authority should be placed in charge of coordination of CIP activities. The functions of the NCCM&CIP should include all those functions that are targeted at addressing CIP system tasks not covered by the existing state-level systems (civil defense, counterterrorism, suppression of cyber-threats, etc.), specifically the functions of coordination (all tasks in this group), decision support (most of such tasks), international cooperation, as well as part of the functions in the other two groups.

CIP tasks shift the focus toward prevention of crises related to CI operation in Ukraine. Note that the definition of a crisis situation is not uniform throughout the Ukrainian legislation. It may be used either in a broad sense: «abrupt escalation of conflicts, acute destabilization of a situation in any area of activity, region, or country» or as a synonym of a politico-military crisis: «a state characterized by the uttermost escalation of regional or international politico-military situation, where opportunities for peaceful settlement of disputes are exhausted and there is a real threat of employment of military force,» or else in a narrow sectoral sense, e.g. for a nuclear facilities and nuclear material

physical protection system: «a situation that has occurred or may occur as the result of sabotage, theft or any other unauthorized removal of nuclear material, or threat thereof.»[10] The definition of a crisis situation has a consequential relation to CI and accounts for impacts of both external security environment factors and factors of operation of the critical infrastructure assets per se. For the avoidance of doubt we are going to provide definition of this term in the meaning that is used in this Green Paper.

A *crisis situation* related to critical infrastructure is a situation involving emergence or escalation of factors, change of conditions or characteristics of security environment, or change of operational status of certain critical infrastructure assets such that it creates a threat for security and/or resilience of CI (or an individual sector or asset thereof).

Thus it is prevention of crises that should become a key component of the functioning of the NCCM&CIP. Potential crises related to CI operation should be continuously monitored and identified. This latter task is achievable provided establishment a unit (department) within the NCCM&CIP that will function as a situation center and promptly and on a 24/7 basis address tasks to support decisions in a CIP system. Specifically, such a division within the NCCM&CIP should interact with (become an integral part to) the network of departmental and corporate situation centers (crisis, information analysis centers etc.) Considering advanced achievements of Ukrainian scientists in the IT sector the task of technology, methodology and human resource support of such a division having the situation center functionality looks quite promising.

The next novelty on the list of CIP system tasks is the idea of an «operation mode» of this system. Note that presently separate operation modes have been identified for state civil protection systems (everyday operation, high alert, emergency situation and state of emergency), suppression of terrorism (by levels of terrorist threat: normal, elevated, high, critical), and physical protection (normal operation, high alert, crisis operation, recovery of normal operation). There is no doubt that operation modes of the above systems are related to the state of CIP.

[10] Regulation of State Nuclear Regulatory Inspectorate of Ukraine of 28 August 2008 № 156. – Retrieved from http://zakon4.rada.gov.ua/laws/show/z1000-08

However, these modes to not correlate with CIP tasks and may not be brought together in a uniform scale in order to formulate critical infrastructure protection system operation modes. Consideration should be given also to the legal arrangements for the regimes of an emergency state[11], an environmental emergency zone[12], and law martial[13] that are also closely related to CIP.

Based on the above and considering the priority of the crisis prevention task for the CIP system, the following modes of this system's operation will be suggested:

- crisis situation prevention (for a single or multiple situations);
- governance in a crisis situation;
- operation in a state of emergency;
- operation in law martial environment.

Under this classification, a normal mode of CI operation will be the mode of crisis risk monitoring and assessment, which is generally aimed for continued prevention of crises. Where a crisis situation could not be avoided, the CIP system should move to the next operation mode, i. e. operation in a crisis situation. Note that a crisis situation may occur in a separate CI sector, however, due to interface between the sectors (interrelations/interdependence of assets pertaining to different sectors) such a crisis may extend to the entire CI and have very serious consequences for socioeconomic development, defense capability or national security of the state.

Governance in a crisis situation mode means the need to apply emergency measures to deter various factors, improve conditions and characteristics of the security environment, improve operation status of individual CI assets, etc. This mode is applied for CI recovery from malicious acts, accidents or failures, or from major impact of hazardous natural phenomena.

Activation of state of emergency or law martial operation modes occurs following the announcement of one of these legal regimes.

---

[11] Law of Ukraine of 16 March 2000 № 1550-III «On the Legal Regime of Emergency State». – Retrieved from http://zakon3.rada.gov.ua/laws/show/1550-14

[12] Law of Ukraine of 13 July 2000 № 1908-III «On the Environmental Emergency Zone». – Retrieved from http://zakon2.rada.gov.ua/laws/show/1908-14

[13] Law of Ukraine of 11 June 2015 «On the Legal Regime of Martial Law». – Retrieved from http://zakon2.rada.gov.ua/laws/show/389-19

Identification of principles for economic relationships and their changes in various operation modes should become an important precondition of CI operation and an element of governance in various modes. Operators and the state should have clear understanding of economic repercussions and responsibility for critical infrastructure protection measures in each of the operation modes. At the same time it should be noted that applicable laws do not fully govern compensation of additional expenses incurred by CI operators amid crisis situations. Lack of clearly formulated responsibilities in case of enhancement of CI asset security status should be addressed through adoption of appropriate regulatory documents.

A *national critical infrastructure protection plan* (NCIPP) is a third novelty. The goal of such a document is a detailed review of the critical infrastructure protection system including both definition of avenues for system development and the general description of specific mechanisms to achieve the system tasks. The NCIPP should specifically focus on *actions to prevent crisis situations*[14] in order to identify mechanisms of detection and mitigation of threats for critical infrastructure (sectors thereof).

The next feature of critical infrastructure protection system tasks to be mentioned is preparation of a *national DBT for critical infrastructure.* At present, the Ukraine's state-level physical protection system provides for the development and periodical updates of a design basis threat actually defining the list of those threats (and their descriptions), which should be accounted for in the physical protection of facilities. Although the physical protection system is targeted to protect only a certain category of assets (nuclear material, nuclear facilities, radioactive waste and other sources of ionizing radiation), a DBT development mechanism is important from the perspective of identification of requirements for a physical protection system and, accordingly, of operator responsibilities in respect of facility security. In our view, the DBT development experience of the nuclear sector may be extended, subject to appropriate adjustments, to other CI sectors.

[14] Say, in the UK the government has developed a National Preventive Plan: Gas for gas supply to the energy sector (see https://www.gov.uk/government/publications/national-preventive-action-plan-gas) in correlation with general European standards implemented by EU Regulation № 994/2010 concerning measures to safeguard security of gas supply.

Subjects of a Critical Infrastructure Protection System

Certainly, the state, through its authorized agencies, should play a key role in the activity aimed for sustainable critical infrastructure security. This primarily applies to the establishment of the appropriate regulatory framework. Role of government authorities is also apparent in the events where CI elements are fully or partly owned by the state.

At the same time, a substantial – and sometimes even prevailing – part of CI assets in many countries are owned privately. Thus, in the Canadian National Critical Infrastructure Strategy (Security), it is emphasized that «chief responsibility for enhancement of CI resilience remains with owners and operators.» In this connection effective PPP in security in general and in CIP in particular are probably the most important component of the government policy in this area.

As for the responsibility for CIP in a state and coordination of relevant activities, international practice proves that different organizational approaches may be viable.

E. g., in the U.S. the Department of Homeland Security established immediately after the 9/11 terrorist attacks is responsible for a considerable number of CI sectors. Canada uses a similar approach: the Ministry of Public Safety and Emergency Preparedness is entrusted with the relevant functions, excepting for the issues of maritime safety.

In Germany, activities related to CIP are coordinated at the state level by the Federal Ministry of Interior whose organization includes appropriate institutions and agencies responsible for assessment of threats for CI, analysis of ongoing security environment and development of CIP concepts.

In the UK, the governmental agency called *Centre for the Protection of National Infrastructure, CPNI, accountable to the Security Service (MI5) Director General,* provides consultancy to private companies and organizations in respect of physical protection of the national infrastructure.

In Poland, coordination of CIP measures is the responsibility of the Government Center for Security, being a super-ministerial organization accountable directly to the Prime Minister. This Center has developed a National Program for Critical Infrastructure Protection.

In Ukraine, CI is not defined on a legislative level, thus there is no CIP subject. In our state, the Integrated System for Prevention of, Response to and Suppression of Terrorist Acts and Minimization of

Consequences Thereof (USSPRM-T) (Provision approved by the Cabinet Decree of 15 August 2007 № 1051), the Unified State System for Civil Protection (USSCP) (Provision approved by the Cabinet Decree of 9 January 2014 № 11), and the State Physical Protection System (SPPS) (Functional Procedure approved by the Cabinet Decree of 21 December 2011 № 1337) function in parallel.

These systems have been established, inter alia, for the protection of vital national assets against certain types of threats, which results in a situation where departmental approach to addressing state-level security issues becomes dominant.

Another issue that awaits resolution is creation of an integrated state system for the detection and prevention of cyber-attacks against the state's critical information infrastructure assets, assessment of the level of security of its elements, mobilization of personnel and equipment for the detection and prevention of cyber-attacks, as well as appropriate control and coordination bodies at various levels, authorized to provide security of CI automatic control systems.

The work toward establishment of a national center for cyber protection and suppression of cyber threats and a national center for operator- and process-enabled control of Ukrainian telecommunication networks has been intensified for objective reasons in the need to support nation's defense capability during a special period (this task is mentioned in the appropriate NSDCU resolution[15]).

In January 2015, the Ukrainian Cabinet Decree № 18 approved the Provision on the State Commission on Technogenic and Ecological Safety and Emergency Situations (the Provision), as well as the composition of commission members. Pursuant to the Provision, the State Commission on Technogenic and Ecological Safety and Emergency Situations (State Extraordinary Commission) shall be a standing body to coordinate the activity of central and local executive authorities directed to assure anthropogenic and environmental safety, protection of the public and territories against consequences of emergencies, and organizational measured to suppress terrorist activity and military threat, prevent and respond to emergency situations.

---

[15] Resolution of the National Security and Defense Council of Ukraine of 28 August 2014 «On Immediate Measures for the Protection of Ukraine and Enhancement of Its Defense Capability». – Retrieved from http://zakon3.rada.gov.ua/laws/show/744/2014

Some of the key tasks of the State Extraordinary Commission are close to critical infrastructure protection goals. They include:

1) coordination of efforts of central and local executive authorities for:

- assurance of resilience of national economy and public administration assets *during emergency response;*
- assurance of stable operation of fuel and energy sector *in an emergency* and of coordinated effort of enterprises, institutions and organizations to secure sustainable and uninterrupted operation of the Gas Transmission System and Integrated Energy System of Ukraine;
- assurance of security and sustainable operation of transport infrastructure, postal and electronic communication services;

2) identification of ways to address problem issues occurring as the result of disruption of proper operation of infrastructure assets and safe vital activity of the public, including in the areas of national security and defense, energy, finance, social protection, and environment.

The above Decree partially provides a formal solution for the coordination of efforts in CIP, however it is only limited to emergencies as interpreted for the civil protection purposes. Due to a number of methodology limitations, the existing civil protection system does not offer a systematic solution for CIP.

Choice of an organizational model for CIP in Ukraine requires an in-depth study of international experience, however, the preliminary analysis suggests that the organizational approach applied in Poland, being our neighbor state, could be acceptable for Ukraine; its frameworks could be used to accommodate some of the Ukrainian developments in establishment of state- and sector-level situation centers that form a national distributed situation center network having information analysis support for the national situation/crisis center as one of its principal functions.

Development of Critical Infrastructure Protection Mechanisms for Ukraine

CIP is a sophisticated and multi-faceted task for any state, however abundant its resources may be. Based on the analysis of experience of the leading nations in protecting national CI and on the assessment of the CIP status in Ukraine we suggest the following key avenues for the development of critical infrastructure protection mechanisms in our state:

- establishment of regulatory and institutional mechanisms for CIP;
- identification of CI priority sectors;
- identification of government authorities responsible for the establishment and implementation of state policy for CIP; clear allocation of responsibilities between all participants of CIP processes/arrangements;
- development and approval of criteria and methods for attribution of assets (irrespective of ownership form) to a CI list;
- improvement of a system for CI asset condition monitoring, CI threat analysis and forecast, identification of methods and ways for CI operation related risk mitigation, enhancement of reliability, resilience and sustainability of CI assets, prevention of emergencies at such assets;
- improvement of PPP mechanisms, identification of CIP funding sources;
- implementation of innovative developments and improvement of existing means for CI assets security and protection;
- development and implementation of standards, regulations and technical conditions for CI asset security;
- implementation of a «risk management culture» in operators' management systems;
- improvement of CI assets protection regimes;
- involvement of expert community and the public, dissemination of information and best achievements, training, exercises and drills;
- elimination of threats, mitigation of threats through application of integrated security arrangements (e. g. as part of the terrorism suppression effort);
- development of international cooperation in CIP.

In order to implement the overall approach to CIP in Ukraine, the following priority steps should be considered.

a) *For regulatory governance of CIP*:

- definition of principal terms («critical infrastructure», «critical infrastructure protection», «critical infrastructure regulator», «critical infrastructure operator», etc.);
- implementation of a CI assets identification procedure (creating a list);
- implementation of a procedure for the change of a CIP system operation mode depending on the level of threat;

- governance of information exchange and data acquisition in respect of CI assets, threats and risks for these assets;

b) *For institutional support of the required arrangements*:

- establishment or nomination of a government authority to bear responsibility for establishment and administrative, technical and scientific support of a national *center for crisis management and critical infrastructure protection* (NCCM&CIP) and for creation and support of a state-level (national) system (network) of distributed situation centers (sectoral centers) based on common interface regulations and uniform methodology and organizational approaches;
- analysis and assessment of operation of existing sectoral situation centers (including their equipment, methodology and human resource base) with a view to create a national network of distributed situation centers having information analysis support for the NCCM&CIP as one of its principal functions;

c) *For organizational, technical, methodology and human resource support*:

- development of a methodology for qualification of assets as CI;
- development of a methodology for identification of condition of CI assets and assessment of effectiveness of emergency response at such assets;
- improvement of monitoring systems, including remote sensing, forecast systems and decision support systems;
- development and implementation of a decision support system for the NCCM&CIP;
- development of recommendations to launch comprehensive target research programs and more intensive involvement of private sector in the funding of CIP research;
- training and retraining of personnel in CIP, organization of special drills and training courses at the existing training centers in the nuclear sector, civil protection sector, etc.;

d) *For the involvement of business sector and the public in addressing CIP issues*:

- raising public awareness concerning the main goals of critical infrastructure assets protection, inter alia to deter potential adversaries;

- organization of PPP in security;
- enabling and stimulation of involvement of private sector operators/owners in CIP;
- support of national manufacturers in the security services market (specifically, in cyber security);
- establishment and support of appropriate consultancy, advisory, etc. teams.

CRITICAL INFRASTRUCTURE IN THE VIEW OF EUROPEAN INTEGRATION COURSE OF UKRAINE AND INTERNATIONAL COOPERATION

Due to its geographical location, Ukraine has especially tight links with energy and transport infrastructure of the Member States. Ukraine is an integral part of the global cyber space. Therefore, taking into account modern geopolitical reality, one should realize that, for example, Ukrainian gas transportation system can be considered by European and Transatlantic partners as a critical infrastructure element of Pan-European importance.

Signature of the political part on March 21, 2014 and of the economic part on June 27, 2014 of the Association Agreement[16], followed by its ratification by Ukraine and by a number of Member States have made it necessary to identify the priority steps, which Ukraine should make in order to put its approaches in this field in compliance with the approaches applied in EU.

In the EU, establishment of legal and organizational mechanisms of CIP was initiated in 2004 by the address of European Council to European Commission, in which European Commission was committed to prepare the general strategy of CIP.

In October 2004, the European Commission published official Communication [18] containing review of Commission's activities in this field and propositions regarding additional measures aimed at improvement of the European System of Prevention of, Preparedness for and Response to Terrorist Attacks Aimed at EU Critical Infrastructure

[16] Association Agreement between Ukraine, on one side, and European Union, European Atomic Energy Community and the member states, on the other side. – Retrieved from https://eeas.europa.eu/sites/eeas/files/association_agreement_ukraine_2014_en.pdf

Elements. This Communication emphasized that approach to critical infrastructure protection in all EU countries should be methodologically similar. European Critical Infrastructure Protection Program (ECIPP) and European Critical Infrastructure Warning Information Network (CIWIN) should ensure implementation of such general approach.

In the official Communication № 786 issued in 2006 [19], European Commission recommended to all EU countries to take measures stipulated in ECIPP, namely:

- develop national CIP program (plan) as a document that has legal effect;
- meet the level of health protection, process safety, social and economic well-being that would ensure nation's «endurance» against threats;
- unify efforts aimed at CIP, by assigning to a single state body who reports on this issue the functions coordinating activities of state authorities, which have special fields of interest and tight relations with industries owing CI facilities;
- identify state authorities responsible for CI sectors and corresponding private companies;
- create conditions for efficient interaction and exchange of information (IEI), data and experience between European Union member states, governmental structures and private sector;
- contribute to creation of harmonized methodology at the level of European Union's and Pan-European risk assessment system.

Propositions regarding the procedure and criteria of identification of CI facilities at the Pan-European level were presented in the Green Paper (2005) [20]. It reviewed 11 CI sectors which included 37 subsectors. Then, during preparation of the Draft Directive, 11 sectors out of 29 subsectors [21] were identified, and the approved European Commission Directive [22] now mentions only two European CI sectors containing eight subsectors:

- power industry (electrical grids and generating and transmission facilities; oil refining industry, oil extracting industry, oil pipelines and depots; gas producing industry, gas pipelines, liquefied gas terminals);
- transportation industry (automobile transport; railway transport; air transport; river fleet; ocean and sea fleets and ports).

At the same time, the Directive does not prohibit identification of national CI in other sectors.

Regarding CIWIN, the main task of this network is generation of tools for IEI on CI at the Pan-European level. CIWIN is characterized by strict requirements to information safety since the network processes information that is sensitive in terms of critical infrastructure facilitiessecurity [23].

So, when developing a CIP system in Ukraine, taking into account European integration course of our country, it is necessary to make efforts in reaching compliance of the national legislation with EU's regulations regarding the following:

- general principles of CIP;
- interpretation of basic terms;
- determination of the «Point of contact».
- compliance in terms of CIP's priority (selection of priority sectors and corresponding subsectors of CI);
- methodology of comparison and identification of priority facilities in various sectors;
- implementation of current European Union's CIP standards.

It is also worth mentioning that in the course of development of a CIP system in Ukraine, one should take into account the fact that according to the Association Agreement the «Early Warning Mechanism» has been already created in Ukraine, with the purpose of early assessment of potential risks and challenges related to demand and supply of natural gas, oil or electricity, as well as in order to ensure warning and prompt response in case of emergency or of threat of emergency.

When developing the national regulatory and legislative framework in the field of CIP, special attention should be paid to the documents aimed at maximum approximation of the national legislation requirements to the requirements of CI operation and protection in the energy and transport industries that are stipulated in the EU Directives and in the Association Agreement between Ukraine and European Union[17]:

- Directive 2005/89/EU of the European Parliament and of the Council Concerning Measures to Safeguard Security of Electricity Supply and Infrastructure Investment;
- Regulation (EU) № 994/2010 of the European Parliament and of the Council of 20 October 2010 concerning measures to safeguard security of gas supply and repealing Council Directive 2004/67/EC;

[17] Annex XXVII to the Association Agreement. – Retrieved from http://eeas.europa.eu/archives/delegations/ukraine/eu_ukraine/association_agreement/index_en.htm

- Directive 2005/65/EU of the European Parliament and of the Council of 26 October 2005 on Enhancing Port Security;
- Regulation (EC) 725/2004 of the European Parliament and of the Council on Enhancing Ship and Port Facility Security;
- Directive 2004/49/EU of the European Parliament and of the Council of 29 April 2004 on Safety on the Community's Railways[18];
- Regulation (EC) 336/2006 of the European Parliament and of the Council of 15 February 2006 on the Implementation of the International security Management Code within the Community[19].

Importance of formation of international framework agreements regarding critical infrastructure protection at the global level should be noted. In this context, preparation by UN expert team of Draft Memorandum of Nonaggression on Critical Infrastructure Facilities Using Information Technologies can serve an example of such initiative. Ukraine should also take an active part to such cooperation forms.

KEY CONCLUSIONS

The Green Paper covered a wide spectrum of issues related to CIP. This Paper combines analysis of the situation in Ukraine regarding solving tasks of protecting individual groups of CI facilities and analysis of experience of CIP system development in the world's leading countries. Not putting aside other issues, we would like to focus attention on the issues that first of all concern generation of the state policy in this field and establishment of a CIP system in Ukraine in the future.

a) Today, CIP is an element of the safety policy, both at the national level of individual EU and NATO Member States and at the international level, in the scope of the above mentioned inter-state union and

[18] Directive 2004/49/EC of the European Parliament and of the Council of 29 April 2004 on safety on the Community's railways and amending Council Directive 95/18/EC on the licensing of railway undertakings and Directive 2001/14/EC on the allocation of railway infrastructure capacity and the levying of charges for the use of railway infrastructure and safety certification (Railway Safety Directive). – Retrieved from http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32004L0049

[19] Regulation (EC) № 336/2006 of the European Parliament and of the Council of 15 February 2006 on the implementation of the International Security Management Code within the Community and repealing Council Regulation (EC) № 3051/95. – Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32006R0336

military and political block. For Ukraine, taking into account complicated security situation, the task of establishment of a CIP system may seem too ambitious. But its gradual implementation will allow enhancing the national security protection system by reinforcing its capabilities of preventing crisis situations related to CI operation. At the same time, implementation of a CIP system will even more approximate domestic management mechanisms in the field of national security to the mechanisms used in European Union and NATO Member States. CIP in Ukraine should become an integral part of Pan-European security mechanism.

b) This Green Paper identifies strategic goals of the state policy in the field of CIP and, correspondingly, CIP system's tasks and CIP establishment principles. In its turn, system's tasks will drive functions of CIP subjects. Establishment of a state CIP system in Ukraine requires introduction of certain changes in the national legislation. It seems reasonable to adopt a separate Law of Ukraine to specify principles of the state policy in the field of CIP in Ukraine, subjects, tasks and structure of a CIP system in Ukraine, to establish responsibilities of the state authorities regarding identification of this system's operation features.

c) The policy of CIP should be based on cooperation between the state and the private sector. Therefore, forming and development of the state-private partnership are critical for the state policy on CIP and it should be regulated by the law, should find methodological, organizational and technical support for coordinated actions. Besides, mutual relations between operators and the state, both in supporting CIP system operation and in exchanging information as per the stipulated requirements will demand regulatory, organizational and technical arrangements in the scope of the state CIP system operation.

d) Partnership means high-level commitments of CI facility operator in terms of facilities security, as well as the regulator's capability to take efficient actions and ensure endurance of the entire CI, especially under conditions of emergency at individual facilities. A separate issue to be solved is arrangement of full-scope funding for CI operators' costs that may additionally arise under conditions of emergency.

e) Particular tasks of CIP that differ from the tasks of the existing state civil protection system, counter-terrorism protection, cyber threat counteraction etc. demand organizational novelties, namely, establishment of NCCM&CIP as a separate body or as a structural part of an

authority to be responsible for coordination of actions on CIP. Such center should coordinate development of legal, organizational, technological and other tools of critical infrastructure protection, organize and involve all stakeholders (operators, regulators, local executive authorities, public etc.) in such development. Specification of CIP system's tasks and determination of its subjects' functions require further discussion of this agenda by the expert community, among government employees, officers of law-enforcement agencies and special services, private sector representatives, all those involved and competent in this issues.

f) While the Green Paper proposes a list of CI sectors along with general structure of criteria of designation of certain facilities as CI facilities, the process of such facilities identification will require regulatory, legislative, organizational and methodological support. It should be noted that none of the existing categories of facilities, for which special protection and operation conditions should be established, has grounds to be fully treated as CI facilities without additional analysis.

Thus, this Green Paper is a step to comprehend integral state policy in the field of CIP on the way of its formation in Ukraine.

Annex A

Propositions on the List of Critical Infrastructure Sectors and responsible authorities[xxi]

Critical infrastructure sector	Main institutions responsible for safety, security and operation of sector's facilities
1. Fuel & Energy Complex	Ministry of Energy and Coal Industry of Ukraine (MoECI), Security Service of Ukraine (SSU)[xxii], Ministry of Internal Affairs of Ukraine (MIA)[xxiii], State Service of Special Communications and Information Protection of Ukraine (SSSCIP)[xxiv]
2. Transport	Ministry of Infrastructure of Ukraine, SSU[xxi], MIA[xxii]
3. Life Support Networks	Ministry of Regional Development of Ukraine, Construction and Communal Services of Ukraine, State Service of Ukraine for Emergency Situations (SESU)[xxv]
4. Telecommunications and Communication Networks	SSSCIP, MIA[xxii]
5. Financial and banking sector	National Bank of Ukraine, Ministry of Finance of Ukraine, SSU[xxi], SSSCIP[xxiii]
6. Public administration and law-enforcement	SSU[xxi], MIA[xxii], State Guard Service[xxii]
7. Security and defense complex	Ministry of Defense of Ukraine (MoD), MIA[xxii], SSU[xxi]
8. Chemical industry	State Service of Ukraine for Labor, SSE[xxiv], SSU[xxi]
9. Emergency services and civil protection	SESU, Ministry of Health of Ukraine
10. Food processing industry and agricultural complex	Ministry of Agrarian Policy and Food of Ukraine

Notes: [xxi]– institutions responsible for adoption of regulatory and legislative acts governing critical infrastructure protection should be specified. [xxii]– in the scope of counter-terrorist activities. [xxiii]– regarding facilities security. [xxiv]– regarding cyber threat counteraction. [xxv]– in the scope of civil defense tasks.

Annex B

Structure of the Draft Law of Ukraine
On Critical Infrastructure

I. General
1. Scope of Law
2. Definitions

II. State Policy on Critical Infrastructure Protection
3. Principles of State Policy in the Field of Critical Infrastructure Protection
4. Purposes of State Policy on Critical Infrastructure Protection
5. Critical Infrastructure Protection Facilities
6. Critical Infrastructure Protection Subjects

III. Critical Infrastructure Protection System
7. Purposes and Tasks of Critical Infrastructure Protection System
8. Authority and Tasks of State Authorities in the Field of Critical Infrastructure Protection
9. Interaction with Other Protection Systems in the Field of National Security
10. Organization of Interaction in the Field of Critical Infrastructure Protection
11. Information exchange in the Field of Critical Infrastructure Protection
12. Changing Operating Modes of Critical Infrastructure Protection Systems Depending on the Threat Level and Legal Status
13. Participation of the Public in Critical Infrastructure Protection

IV. Mechanisms of Critical Infrastructure Protection Policy Implementation
14. Criteria and Methodology of Designation of Facilities as part of Critical Infrastructure Facilities List
15. System of Critical Infrastructure Facilities Status Monitoring, of Critical Infrastructure Threat Analysis and Forecasting
16. Determination of and Notification on Critical Infrastructure Threat Level

LIST OF REFERENCES

1. Decree of the Cabinet of Ministers of Ukraine of 23 December 2004 № 1734 «On Approval of List of Enterprises That Are of Strategic Importance for National Economy and Security». – Retrieved from http://zakon5.rada.gov.ua/laws/show/1734-2004-%D0%BF

2. Decree of the Cabinet of Ministers of Ukraine of 28 July 2003 № 1170 «On Approval of List of Critical Electrical Power Facilities That Must Be Guarded by Corporate Paramilitary Security in Interaction with Special-Purpose Units of Other Central Executive Bodies». – Retrieved from http://zakon.rada.gov.ua/go/1170-2003-%D0%BF

3. Instruction of the Cabinet of Ministers of Ukraine of 27 May 2009 № 578-p «On Approval of List of Critical Oil and Gas Industrial Facilities». – Retrieved from http://zakon2.rada.gov.ua/laws/show/578-2009-%D1%80

4. Decree of the Cabinet of Ministers of Ukraine of 15 August 2007 № 1051 (confidential).

5. Provision on Integrated System for Prevention of, Response to and Suppression of Terrorist Acts and Minimization of Consequences Thereof (ap proved by the Decree of the Cabinet of Ministers of Ukraine of 15 August 2007 № 1051). – Retrieved from http://zakon2.rada.gov.ua/laws/show/92-2016-%D0%BF

6. Decree of the Cabinet of Ministers of Ukraine of 24 April 1999 № 675–019 «On Approval of List of Objects to be Guarded and Defended in Emergency and During Special Period».

7. Decree of the Cabinet of Ministers of Ukraine of 10 August 1993 № 615 «On Measures on Improvement of Security for Assets of State and of Other Type of Property». – Retrieved from http://zakon.rada.gov.ua/laws/show/615-93-п

8. Law of Ukraine of 18 January 2001 № 2245 «On Extremely Dangerous Facilities». – Retrieved from http://zakon.rada.gov.ua/laws/show/2245-14

9. List of Extremely Dangerous Facilities Disruption of Which Requires Special Measures on Prevention of Damage to Lives and Health of the Public, to property, to structures, to Natural Environment / Approved by the Decree of the Cabinet of Ministers of Ukraine of 06 May 2000 № 765. – Retrieved from http://zakon.rada.gov.ua/laws/show/765-2000-п

10. Decree of the Cabinet of Ministers of Ukraine of 29 August 2002 № 1288 «On Approval of the Provision on the State Register of Potentially Dangerous Facilities». – Retrieved from http://zakon.rada.gov.ua/laws/show/1288-2002-п

11. Order of SNRIU of 17 December 2012 № 238 «On Approval of List of Radiological Hazardous Facilities in Ukraine, for Which Facility-Level Design Basis Threat Should Be Developed».

12. Decree of the Cabinet of Ministers of Ukraine of 02 March 2010 № 227. – Retrieved from http://zakon.rada.gov.ua/laws/show/227-2010-п

13. Approved by the Decree of the Cabinet of Ministers of Ukraine of 09 January 2014 № 6. – Retrieved from http://zakon.rada.gov.ua/laws/show/6-2014-п

14. Law of Ukraine of 13 March 2012 № 4499 «On the System of Public Emergency Care Via Single Telephone Number 112». – Retrieved from http://zakon2.rada.gov.ua/laws/show/4499-17

15. Law of Ukraine of 10 January 2002 № 2919I «On the National Confidential Communication System». – Retrieved from http://zakon2.rada.gov.ua/laws/show/2919-14

16. Law of Ukraine of 05 April2001 № 2346 «On Payment Systems and Money Transfer in Ukraine». – Retrieved from http://zakon5.rada.gov.ua/laws/show/2346-14

17. Law of Ukraine of 08 June 2000 № 1805 «On Cultural Heritage Conservation». – Retrieved from http://zakon3.rada.gov.ua/laws/show/1805-14

18. Communication from the Commission to the Council and the European Parliament of 20 October 2004 – Critical Infrastructure Protection in the Fight Against Terrorism (COM/2004/702 final). – Retrieved from http://eur-lex.europa.eu/

19. Communication from the Commission on a European Programme for Critical Infrastructure Protection (COM/2006/786 final). – Retrieved from http://eur-lex.europa.eu/

20. Green Paper on a European Programme for Critical Infrastructure Protection (COM/2005/576 final). – Retrieved from http://eur-lex.europa.eu/

21. Proposal for a Directive of the Council on the Identification and Designation of European Critical Infrastructure and the Assessment of the Need to Improve Their Protection (COM/2006/787 final). – Retrieved from http://eur-lex.europa.eu/

22. Council Directive 2008/114/EC «On the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection». – Retrieved from http://eur-lex.europa.eu/

23. Commission Staff Working Document – Accompanying Document to the Proposal for a Council Decision on Creating a Critical Infrastructure Warning Information Network (CIWIN) – Impact assessment (SEC/2008/2702). – Retrieved from http://eur-lex.europa.eu/

1.2. THE DECREE OF PRESIDENT OF UKRAINE AND THE DECISION OF THE NATIONAL SECURITY AND DEFENSE COUNCIL OF UKRAINE

The Decree of President of Ukraine № 8/2017[20]

On the decision of the National Security and Defense Council of Ukraine «On improvement of measures to ensure the protection of critical infrastructure objects»

According to article 107 of the Constitution of Ukraine, **I decree**:

1. To put into effect 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» (attached).

2. The Secretary of the National Security and Defense Council of Ukraine is to follow up on implementation of the decision of the National Security and Defense Council of Ukraine put into effect by this decree.

3. This Decree enters into force at the day of its publication.

President of Ukraine **P. POROSHENKO**
16 January 2017

---

[20] The unofficial translation.

Put into effect
by Presidential Decree
of 16 January 2016 № 8/2017

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

Having considered the status of implementation of priority objectives of the state policy in the field of national security of Ukraine with regard to critical infrastructure security identified in the Ukrainian National Security Strategy, approved by Presidential decree of 26 May 2015 № 287, in order to ensure comprehensive improvement of a legal basis for critical infrastructure protection and to establish a state administration system for its security the National Security and Defense Council of Ukraine adopted the following **decision:**

1. the Cabinet of Ministers of Ukraine shall:

1) within two months draft with the participation of the National Institute for Strategic Studies and approve the concept of establishing the state critical infrastructure system and the working plan for its implementation;

2) within two months after approval of the concept of establishing the state critical infrastructure 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 established procedure to submit the draft law to the Verkhovna Rada with the aim to legislatively resolve, inter alia, the following issues:

establishing the state critical infrastructure protection system;

identifying an authority responsible for coordination of activities aiming at the critical infrastructure protection both in peace time and in the special period of time;

identifying the functions, powers, and responsibilities of the central executive authorities and other organizations concerning critical infrastructure protection as well as rights, obligations and responsibilities of the owners and operators of the critical infrastructure objects;

introducing common methodological approaches to assessment of threats to critical infrastructure and to response activities including to accidents and technical failures, natural hazards, malicious actions;

introducing criteria for and a methodology of infrastructure objects assignment to critical infrastructure, procedures for such objects security certification and categorization;

laying foundations for the public-private partnership and providing resource support in the field of critical infrastructure protection;

ensuring international cooperation in the field of critical infrastructure protection.

2. The Security Service of Ukraine within three months shall take measures to improve counterintelligence support to critical infrastructure protection.

Secretary of the National Security and Defense Council of Ukraine **O. TURCHYNOV**

1.3. THE CONCEPT FOR BUILDING A STATE CRITICAL INFRASTRUCTURE PROTECTION SYSTEM IN UKRAINE

(DRAFT[21])

I. THE PROBLEM TO BE SOLVED

Raising awareness of the current world tendencies of increased numbers of natural and man-made disasters, terrorist acts, sophisticated cyber-attacks which are especially strengthened in eastern and southern Ukraine due to Russian Federation's aggression accompanying with numeral damages of infrastructural objects has made it urgent for Ukraine to provide necessary protection of systems, objects and resources which are critically important in terms of society stable functioning, social and economy development and national security.

When doing so, it is necessary to take into account that the most dangerous for CI operation are those threats which realization at one object due to various interconnections could cause crisis situations at the similar objects (a domino effect) and/or at objects of other types (a cascade effect).

At present, there is a number of separate state/national systems in Ukraine which functions according to modern approaches could be related to the critical infrastructure protection (CIP). Among them the following should be noted:

The Unified State System for Civil Protection (USSCP)[22];

---

[21] Unofficial translation of the draft concept submitted by the NISS to the Cabinet Ministers of Ukraine (March, 2017) in pursuance of the relevant NSDCU's decision put into effect by Presidential decree of 16 January 2017.

[22] Resolution of the Cabinet of Ministers of Ukraine of 9 January 2014 № 11 «On approval of Provision on the Unified State System of Civil Protection». – Retrieved from http://zakon.rada.gov.ua/laws/show/11-2014-п

The Unified State System for prevention of, responding to and suppressing terrorist acts and mitigation their consequences (USSPRM-T)[23];

The State Physical Protection System (SPPS)[24].

Besides, in pursuance of the Cyber Security Strategy of Ukraine approved by the Presidential Decree of 15 March 2016 № 96/2016, *the National Cyber Security System (NCSS)* is creating which objectives are tightly connected with the CIP.

The severity of the CIP problem in Ukraine is essentially due to the fact that none of the listed above systems is designed to respond to all types of threats and hazards. That is why one could observe the lack of a systematic approach at the national level required for the CIP which would provide possibility to take into account numerous links and interrelations among its elements. Besides, at the moment, no one Ukrainian authority is held fully responsible for the CIP, as a whole.

Thus, basing on the national security needs as well as necessity to apply a systematic approach to solve the problem of CIP at the national level, the establishment of the a CIP system should be recognized as one of the priorities in reforming national security sector of Ukraine at this point of time.

Currently, the key challenges in terms of CIP system establishment at the national level are the following:

- Insufficiency and inconsistency of the legislative framework for protection of objects and systems that should be assigned to critical infrastructure and, in particular, the absence of a law on CI and its protection;
- The absence of a national authority responsible for coordination and interaction in the field of CIP including the national/state systems designed to ensure protection of various objects and response to crises of different origins;
- The lack of clear lines of power and responsibility among central executive bodies and other agencies with regard to CIP, as

[23] Resolution of the CMU of 18 February 2016 № 92 «On approval of the Provision on the unified state system of prevention, response and suppress of terrorist acts and to minimize their effects». – Retrieved from http://www.kmu.gov.ua/control/ru/cardnpd?docid=248852549

[24] Resolution of the CMU of 21 December 2011 № 1337 «On approval of the Provision on functioning on the State Physical Protection System». – Retrieved from http://zakon0.rada.gov.ua/laws/show/1337– 2011-%D0%BF

well as well-defined rights, duties and responsibilities of CIP owners (operators);

- The absence of a nation-wide recognized methodology for threats and risk assessment;
- The lack of common criteria and a methodology to assign objects/systems to CI as well as a methodology of such objects/systems passportization and classification depending on threats and hazards to them;
- The absence of a national law enforcement/intelligence agency responsible for an analysis and assessment of threats to critical infrastructure resulted in the economic field, prevention of and responding to economic threats realization;
- Poor public-private partnership (PPP) in the national security field and uncertainties regarding the sources of funding CIP activities;
- An insufficient level of international cooperation of Ukraine in this field.

Delay in addressing the above issues not only will hinder the process of CIP system establishment but also make obstacles for development in other domains of the national security sector.

Establishment of a state CIP system requires legislatively defining its fundamental principles of operation, application of common approaches to management of CI security at all levels, clear identification of the principles of interaction and cooperation among state authorities, private business, society and public.

Improvement of the national legislative and normative basis for CIP shall be based on unified approaches, a single methodological and terminological basis recognized by all parties involved in state CIP system operation. To facilitate achievement of this purpose the Concept defines the basic terms in the field of CIP.

As used in the Concept:

1) ***Critical infrastructure*** means a set of objects which are so vitally important for ensuring national security and national economic security, for providing essential functions of and services to the Ukrainian society, economy and public, that their destruction or damages would lead to impossibility to maintain the above mentioned functions and to provide the above mentioned services that may be harmful for the national interests of Ukraine.

2) ***Critical infrastructure object*** means an object, system or resource (physical or virtual) assigned to critical infrastructure.

3) ***Subjects of the State Critical Infrastructure Protection System*** mean owners (operators) of a critical infrastructure objects including state bodies, local authorities, management bodies of armed forces established according to Ukrainian legislation, as well as law enforcement bodies.

4) ***Critical Infrastructure Sector*** means a set of critical infrastructure objects having a common functionality.

5) ***Critical Infrastructure Protection*** means a set of organizational arrangements, legislative and regulatory acts, engineering and technical measures, etc., aiming at ensuring critical infrastructure security and resilience through reduction of threats, vulnerabilities and risks, and possible consequences of security incidents minimization.

6) ***Critical Infrastructure Safety*** means a state of critical infrastructure when influence of external and internal factors does not lead to accidents or other deviations in operation during its functioning.

7) ***Critical Infrastructure Security*** means a state of critical infrastructure when it is capable to withstand threats caused by malicious actions against critical infrastructure including cyber-attacks.

8) ***Critical Infrastructure Resilience*** means a state of critical infrastructure under which it is capable to reliably operate under normal operation conditions, able to adapt to continuously changing security and safety environments, to withstand threats and hazards and to rapidly restore after a crisis of any origin.

9) ***Category of Critical Infrastructure Object Criticality*** means a category of criticality of a critical infrastructure object determined basing on its importance, degree of impact on society and State institutions, national economy and defense complex, vital activities of population.

10) ***Critical Infrastructure Objects Categorization*** means a procedure of assigning relevant objects to one of criticality categories.

11) ***Safety and Security Data Sheet (passport)*** means a document of the prescribed by the Cabinet of Ministers' form which contains structured data on a specific critical infrastructure object and specifies a set of measures to be taken by an owner (operator) of the object to protect the object (data included in the document may be assigned to sensitive ones, i. e. those that contain information for official use or commercial secrets, or state secrets.

12) ***Crisis Situation*** means a situation occurring at a critical infrastructure object and/or at interrelated objects (sectors) as a result of a triggering event led to failures in critical infrastructure operation, responding to which requires involvement of external responding forces and resources.

II. THE PURPOSE AND THE TIME-FRAME OF IMPLEMENTATION

The Concept for building a state CIP system (the Concept) defines the principles and objectives of such a system building as well as mechanisms of its operation.

Stable and secure existence of the State, society and public relies on operation of numerous infrastructure objects, systems and networks, as well as on possibility to have an unimpeded access to important resources. The part of such objects, systems and resources is so important for society, economy and the State, that their destruction or damage will lead to negative consequences at the national and, even, global levels. These particular objects, systems and resources are assigned to CI, and to protect them is recognized as a top-priority goal for a modern efficient state.

Ukraine found itself under severe conditions of growing terrorist and cyber-threats, increasing number of natural and man-made disasters that requires to assign CIP to the most important directions of counteracting the threats to national security.

The Concept's goal is to specify the main directions, tools and terms for comprehensive legislative regulation of activities aiming at CIP and establishment of state management system in the field of CIP and resilience against all types of threats including natural, man-made, malicious acts and any combination of the above mentioned.

The Concept is developed in pursuance of the National Security and Defense Council's decision «On improvement of the measures to ensure protection of critical infrastructure objects» of 29 December 2016 put in force by the Presidential Decree of 16 January 2017.

The Concept is based on the provisions of the National Security Strategy of Ukraine approved by the Presidential Decree № 287/2015 of 26 May 2015; takes into account the provisions of the Cyber Security Strategy of Ukraine approved by the Presidential Decree № 96/2016 of 15 March 2016 as well as the provisions of U.N. Security Council Resolution 2341 (2017) «On protection of critical infrastructure against

terrorist acts», S/RES/2341 (2017). Besides, the Concept uses the developments of the Green Paper on Critical Infrastructure Protection in Ukraine (2016) prepared using the best experience and approaches of NATO and EU member States.

It is expected that the Concept implementation will take up 10 years (from 2017 to 2027). However, the pace of the Concept implementation will be obviously dependent on the overall dynamics of reforming the national security sector, as a whole. At the same time, succeeding in building up a state CIP system will help in advancing the general process of reforms through introduction of modern methods to manage security risks at all levels, use of foreign best practices and up to date approaches to protection of CI.

Taking into account diversity and complicated character of the objectives to be accomplished within the framework of the Concept implementation, it is reasonable to divide them into following categories (depending on the terms of implementation):

1. The short-term (priority) objectives (implementation time-lines up to 2 years);
2. The mid-term objectives (3–5 years);
3. The long-term objectives (5–10 years).

Among the short-term objectives are development and approval of the basic legislative and relevant regulations, which will create the foundations for state CI system functioning, including a competent authority determined by the law to coordinate activities aiming at CIP under peaceful conditions and during a special period of time.

Further, among those to be assigned to mid-term objectives creation of organizational and legal as well as functional and structural foundations for establishing the state CI system.

Long-term objectives achievement provides for completion of creation and maintenance efficient operation of the state CI system. Implementation of the Concept will be carried out under short-term and mid-term working plans.

III. THE WAYS AND METHODS TO RESOLVE THE PROBLEMS

The problems of ensuring CIP will be addressed by means of creation of a comprehensive legislative and regulation basis for relevant activities of the authorities, state and private companies; establishment of

the organizational structure for state critical infrastructure protection operation; identification of power and responsibility distribution as well as missions among the subjects of the CIP process.

Legislative and regulatory basis creation for the CIP

The Concept specifies the principal objectives and priority directions of legally regulated activities aiming at ensuring protection and resilience of national CI to guarantee providing public, society, national economy and the State with vital goods and services at a minimum required level within a certain period of time under any conditions.

When creating a legislative and regulatory basis for CIP the principal objective is to establish the system of state control and regulation of the interrelations of authorities, society, operators (owners) of CI, and people with the aim to provide for:

- Critical infrastructure steady operation;
- Its ability to withstand destructive factors and to prevent irreparable damages to its objects and interruption of their operation due to any factors;
- Speedy recovery of its functioning after operation interruption.

The Concept is based on awareness that CIP is the common goal for the State, infrastructure owners (operators), the society and the public assuming from that the following things are required:

- Reliable partnership among the State, business, industry, the society and the public at all levels;
- Striking a balance and achievement of proportionality between requirements to improve the level of protection and costs needed to meet these requirements.

To achieve these objectives the *risks management culture* shall be introduced as one of the pillars of the state CI system operation. Its introduction provides for the following:

- Efficient interaction among the subjects of CIP;
- Improvement of own capabilities of public, owners (operators), organizations and authorities which might be vulnerable to interruptions or deterioration of CI operation;
- Design, construction and operation of CI objects taking into account requirements (technical, administrative, operational, etc.) to ensure their reliable functioning in different modes;

- Introduction of a planning system for responding to crisis situations encompassing all levels of management (state, local, company and organization levels);
- Maintenance of interaction and exchange information (IEI) among all parties involved in CIP against threats and risks of any origin;
- The due level of international cooperation and interaction with foreign partners in the field of CIP bearing in mind global and regional security processes and trends.

The priority directions in development of the legislative and regulatory basis for a state CIP system are:

- establishment of an effective system for state management of the CI in Ukraine;
- ensuring unified methodological foundations for relevant activities carried out by all parties involved in operation of a state CIP system;
- development of regulations on technical requirements for critical infrastructure objects design, construction and operation as well as their stable functioning in different modes;
- establishment of PPP aiming at improvement of security and resilience of national CI that provides for clear legislative regulations on responsibilities and duties distribution among authorities and owners (operators) of the CI objects;
- creation of an efficient system designed for gathering information on threats and risks against CI, its analysis and processing, IEI among all subjects of the process including that addressing responding to crisis situations at the CI objects.

It is anticipated that systemic legal regulation of state CIP system operation will be provided upon the Law of Ukraine «On Critical Infrastructure and Its Protection» approval.

Institutional and organizational framework of a state CIP system

The state CIP has a multilevel architecture reflecting its scale and numerous vertical and horizontal interdependencies existing among CI sectors or its specific objects as well as the complex character of the objectives to be attained.

In order to achieve efficient functioning of a state CIP system provisions will be made to establish a relevant legislative and regulatory basis and to undertake adequate institutional and organizational measures including, in particular, the following:

1. *At the national level (including but not limited to)*:

- Appointment of an authority responsible for shaping and implementation of State's policy in the field of CIP under peaceful conditions and in a special period of time;
- Laying foundations of PPP basing on mutual trust, a due level of information exchange, making the stimuli to invest in CI security, application by the State a balanced approach regarding requirements to improve the level of CIP and costs needed to meet them;
- Functions, powers and responsibilities distribution among of all agencies involved as well as critical infrastructure owners (operators);
- Organization of IEI of all state parties involved in operation of a state CIP system regarding threats and risks to CI, national situation and crisis centers network development;
- Establishment of a national training and re-training system for CIP;
- Development and approval of the CI sectors list and charging specific agencies with responsibility for their protection;
- Establishment a set of operating modes for a state CIP system and transition procedures for them depending on changes in security and safety environment;
- Development and approval of a unified methodology for assessment of threats and risks regarding CI;
- Development, approval and introduction of the methodology for assigning infrastructure objects to CI as well as procedures of their pasportization and categorization; pasportization and categorization of the CI objects;
- Development, approval and introduction of the list and categories of CI objects;
- Establishment of requirements for planning measures to protect CI including emergency plans, plans of interaction, plans for restoration of operation, training (exercise) plans, etc.;
- Development and approval of the national critical infrastructure protection plan (NCIPP).

2. *At the regional and branch levels (including but not limited to)*:

- Development of proposals on particular infrastructure objects assignment to CI;
- Gathering, summarizing and preliminary analyzing of information on CI objects and their performance;

- Maintenance of operation of the relevant IEI systems, monitoring security and safety conditions at the CI objects;
- Participation according to legislative and regulatory acts in responding to crisis situations relating to security and safety of the CI objects and their resilience;
- Early informing (warning on threats) owners (operators) of the CI objects as well as information, advisory, technological and other support to their owners (operators) and consumers (public) to raise preparedness, capabilities to withstand threats and to minimize potential consequences of threats realization;
- Development and introduction of standards, operation regulations aiming at CIP in particular sectors of CI including engineering and technical measures of civil defense for bridge building and project documentation;
- Carrying out public oversight and control measures and assessment of physical security of the CI objects;
- Development and implementation of sector programs to counteract insider threats including through implementation of measures aiming at improvement of security culture;
- Carrying out checks and assessments of information and cyber security at the CI objects;
- Development of regulations to introduce technical requirements for designing, construction and operation of the CI objects (including those providing for implementation of engineering and technical measures for civil defense in bridge building and project documentation) bearing in mind necessity to ensure their stable functioning in different modes;
- Participation in security and safety passports approving and their accounting, as well as in approving and accounting risk maps of different territories and other jurisdictions, etc.

3. *At the local level (including but not limited to)*:

- Development of local programs aiming at CI protection and resilience;
- Development, approval and implementation of local interaction plans for all parties involved, critical infrastructure recovery plans;
- Development, approval and implementation of local programs aiming at improvement of local communities' preparedness for crisis situations resulted from interruption in or deterioration of providing vitally important services and access to critical resources, etc.;

- Designing, development and implementation of engineering and technical measures of civil defense in bridge building and project documentation when considering critical infrastructure objects placing, designing and operation.

4. *At the object level (including but not limited to)*:

- Development and implementation of measures with the purpose of crisis situations prevention;
- Development and implementation of object plans in pursuance of national plans for CIP and resilience;
- Development and implementation of engineering measures for civil defense when designing, constructing and operating CI objects to provide for their stable functioning in different operating modes;
- Creation of material reserves sufficient for object protection plans implementation;
- Development, implementation and revision of objects programs for the purposes of security culture improvement, counteraction to insider threats as well as improvement of cyber and information security;
- Ensuring confidentiality of information according to the requirements laid down by law when processing data on CI objects;
- Ensuring recovery of CI functionality in case of emergencies/failures in operation, malicious acts, natural disasters and any combinations of the above mentioned.

A state CIP system provides efficient operation of the CI in the following modes:

- normal operation mode (threat anticipation and prevention);
- responding to emerging threats (threat determent and CI protection);
- responding to crisis situations (response and suppression);
- consequences mitigation (CI operation recovery).

In order to determine the level of requirements for protection of CI, distribution of powers and responsibilities among all parties involved the procedure of assigning objects to one or another infrastructure category shall be performed within the framework of state CIP system operation.

These categories are the following:

- *Category I*: the objects critically important for the state and having national importance, multiple and complex ties with other infrastructure objects. These objects are to be put on the list of the critical infrastructure objects protection of and resources allocation for which shall be provided according to the legally determined requirements;

- *Category II*: the objects critically important at the regional level. Their destruction and damage will lead to the crisis situations of regional level;
- *Category III*: the important infrastructure objects;
- *Category IV*: necessary infrastructure objects.

Definition of terms «category II», «category III», and «category IV» and establishment of procedure to assign infrastructure objects these categories shall be regulated by the Cabinet of Ministers of Ukraine.

To establish an efficient state CIP system in Ukraine it is necessary to charge certain authorities with responsibility for individual CI sectors to which, first of all, shall be assigned the fuel and energy complex, transport, vital service systems, IT-sector, chemical sector, food industry, banking and finance sector.

Distribution of responsibilities, missions and powers of stakeholders of a state CIP system will be defined by the Law of Ukraine «On Critical Infrastructure and Its Protection», which addresses the following major issues:

- Establishment of a state CIP system;
- Designation of a central authority responsible for coordination of activities aiming at CIP under peaceful conditions and in under special period of time[25];
- Distribution of functions, powers and responsibilities among central executive authorities, other agencies in the field of CIP, as well as rights, duties and responsibilities of CI objects owners/operators;
- Powers of the parts of the national security and defense sector which shall make provisions for maintenance of defense, executing law enforcement, intelligence and counter-intelligence activities, CI counter-terrorist and cyber protection activities, protection of nation economic and technological potential, IEI on threats assessment and responding to security incidents and crisis, as well as crisis management and mitigation of crisis consequences in cooperation with other stakeholders of a state CIP system;

[25] According to best available world practice it might be reasonable to establish a National center for crisis management and critical infrastructure protection (NCCM&CIP) as an executive authority charging with responsibility for CIP system operation, coordination of other state/national systems activities with regard to CIP; development of a unified methodological basis; support to relevant interaction and exchange information (IEI) among all stakeholders; oversight of compliance with legislative requirements for CIP.

- Introduction of a unified methodology for assessment of threats to CI of any origination; establishment of criteria and a methodology for assigning infrastructure objects to critical infrastructure, procedures for infrastructure objects categorization and passportization;
- PPP establishment and development including public-private cooperation in providing due resources for CIP;
- International cooperation in the field of CIP.

IV. EXPECTED RESULTS

The major result of the Concept implementation will be establishment of a state CIP system that can provide a due level of CIP in Ukraine against all types of threats as well as efficient responding to security incidents and crisis associated with CI, consequences mitigation and quick recovery of CIP objects operation relying upon robust interaction, the adequate levels of cooperation, IEI among all stakeholders of the state critical infrastructure protection system, well-developed and sustainable PPP, adequate training and education capabilities and involvement in international cooperation in this field.

A built state CIP system will mean the transition to a qualitatively new level of state management in this field basing on modern approaches to security risks management, the optimum use of available resources, flexibility and timely responding to security and safety incidents and crisis due, in particular, active support from society, local communities, media and NGOs involved in resolving national security and defense issues.

Besides, establishment of a state CIP system will make Ukraine essentially closer to the security standards and regulations applied in the developed states, harmonize Ukrainian legislation in this field with that of EU and NATO, facilitate international cooperation of Ukraine and strengthen Ukraine's potential for integration.

V. FUNDING FOR CONCEPT IMPLEMENTATION

It is anticipated that measures towards implementation of the Concept will be funded from the State budget, by the owners/operators of the CI objects and other sources which are not prohibited by the Ukrainian legislation.

PART II
CRITICAL INFRASTRUCTURE PROTECTION CONCEPT INTRODUCTION: PROCESS AND CHALLENGES

2.1. INTRODUCING THE CRITICAL INFRASTRUCTURE PROTECTION CONCEPT IN UKRAINE: LESSONS TO LEARN

The terrorist attacks against the U.S. on 11 September 2001 showed inadequacy of the security systems both at national and global levels to the sharply increased threats of terrorism and extremism, and forced the international community to cardinally reconsider security approaches worldwide. One of the most important results of such reconsideration was enhanced attention the developed nations began to pay to protection of their critical infrastructure (CI). Following the U.S., a pioneer in this field, a number of nations, first of all NATO and EU member-states, put on the priority list a challenging goal – to protect critically important for them systems, objects and resources against terrorist and other, more traditional, threats such natural disasters and man-made catastrophes and their combinations.

As for Ukraine, our country's security sector since our nation gained independence until the recent crisis was mostly remaining under conditions of stagnation or, even, degradation. That is why its structure, agencies' and bodies' responsibilities and authorities as well as conceptual approaches to respond to modern threats and challenges to national security were far from required ones. Thus, efforts to introduce the concept of critical infrastructure protection (CIP) in Ukraine were started practically from scratch.

When considering the current situation in Ukraine, undoubtedly, our main concerns are connected with the human costs of the crisis which has led to about 6,500 people killed and 16,000 wounded[26].

[26] Information of UN Office for the Coordination of Humanitarian Affairs. – Retrieved from http://www.unocha.org/top-stories/all-stories/five-things-you-need-know-about-crisis-ukraine

Another important aspect of the crisis is the severe humanitarian situation directly connected with the damage and destruction of CI systems and objects, first of all those providing water and energy supply. At this point, bearing in mind that after violence cessation the urgent steps will be addressed to restore, first of all, services and functions vitally important to public health, safety and security, state governance, economy, etc., understanding a CI idea will be of use as well.

This paper outlines the first steps made by Ukraine to introduce CIP concept, analyzes the difficulties and obstacles Ukrainian experts and public servants faced as well as experience gained on this way.

First step: *creation of the interagency expert working group*

Despite Ukrainian political leaders repeatedly stated about Ukraine's choice one day to join the European community in the field of CIP nothing was made to approach Ukrainian legislation to EU's one not saying about practical steps, and by the beginning of 2011 nobody could find the term «critical infrastructure» in the Ukrainian laws and regulations, as opposed to the NATO- and EU-member-states where CIP protection had been intensively developed since 9/11. Thus, in this field by 2011 Ukraine could found itself behind the nations mentioned by, at least, 10 years.

The first practical step to catch this gap was made in March 2011 when the Interagency Expert Working Group (IEWG) on WMD Nonproliferation, Counterterrorism & Critical Infrastructure Protection was established at the National Institute for Strategic Studies. CIP and related issues has become one of the principal subject areas the IEWG addressed in its activities. More than a third of all events carried out by the IEWG were directly devoted to CIP, including international conference on CIP protection (September 2013) carried out with and sponsored by the PDP of the NATO Liaison Office in Ukraine. Besides, a number of problems discussed at the IEWG's meetings considered the issues (e.g. combating nuclear and radiological terrorism, threats and risk assessment in nuclear security area) were also relevant to CIP.

At this stage the NISS's team faced mostly alert colleagues' attitude which was based on the following:

- misunderstanding of the CI idea;
- doubts regarding whether or not Ukraine being in poor economic condition and suffering from lack of funding for cardinal reforms in all sectors was needed to implement such a concept;

- attempts to incorporate a would-be CIP system into existing state ones dealing with either civil defense (response to emergencies) or combating terrorism, etc.;
- just reluctance to change anything connected with their status, duties, authorities, etc.

Nevertheless, the NISS team continued its efforts including making presentations at the meetings and conferences, publication of papers on a subject matter and so on. The situation concerning CIP began getting more favorable, but a real turnaround occurred when the NISS decided to seek support from the PDP of NATO Liaison Office in Ukrainian on this particular issue. Our experts were informed about CIP as one of the priorities in NATO activities named as «protecting Allied nations' critical infrastructure». When persuading our Ukrainian colleagues in importance of the CIP we often referred to the NATO's and EU's efforts and argued that it would be impossible to join one day either of these organizations without harmonizing Ukraine's security approaches (including that CIP was based on) with Alliance's and European ones.

The NISS bilateral cooperation with the PDP of NATO Liaison Office began its development and the next landmark of it became the international conference on subject matter which was arranged by NISS jointly with and sponsored by the PDP.

***Second Step*:** *International Conference on CIP*[27]

The original idea was to carry out an enlarged meeting of the IEWG focused on the CIP inviting NATO member-states' experts to share experience of their countries concerning CIP concept introduction and further implementation. Then we understood that it would be reasonable to transform the group's meeting into a conference essentially expanding the number of Ukrainian participants to promote CIP idea popularization. And the NISS was supported by the PDP with this regard. Later on one more organization – Public Company «Ukrhidroenergo», the largest hydroelectricity generating company of Ukraine, joined to the NISS and PDP to organize the conference. Its active involvement provided participants with opportunity to have the technical tour of the Kyiv Hydroelectric Power Station (Vyshgorod,

[27] International scientific and practical conference «The concept of protection of critical infrastructure: the state, problems and prospects of its implementation in Ukraine». – Retrieved from http://www.niss.gov.ua/articles/1349

Kyiv oblast) and to familiarize with security measures taken at the PC «Ukrhidroenergo».

As for foreign participants of the conference, the NISS was especially interested in involving experts and public servants from Eastern Europe, but other nations' experience was also of great use. And the PDP team dealing with conference arrangements succeeded in inviting proper people from such countries as Bulgaria, Finland, Hungary and Poland. The conference was carried out at two venues – the NISS (Kyiv) and PC «Ukrhidroenergo».

In total, 50 participants took part at the two-day conference, represented four NATO member-states and the PDP. 15 papers on different issues related with CIP were presented. In my view, one of the most useful outputs of the conference in terms of CIP concept introduction in Ukraine was that the majority of participants understood that:

- CIP is an actual direction in ensuring national and international security in NATO and EU member-states, and Ukraine should pay much more attention to this issue;
- NATO would continue support Ukrainian organizations efforts to introduce the CIP concept in our country.

Third Step: *Development and Presentation of the Green Paper on Critical Infrastructure Protection in Ukraine*

Despite some progress achieved by the NISS to facilitate the CIP concept promotion in Ukraine the main obstacle for further steps was not overcome. The case in point was that in our country by that time the bureaucratic practice established not to deal with something if it was not mentioned in Ukrainian legislation. Thus, the problem was to involve authorities in efforts to promote the CIP concept in Ukraine not having even a definition of the term «*critical infrastructure*» in the national legislation. The NISS team decided that the way out of this situation could be found in our developing cooperation with NATO.

After a number of consultations the NISS put forward a proposal to include the item on development of the Green Paper on Critical Infrastructure Protection in Ukraine (GP) in the Annual National Programme of Ukraine-NATO cooperation for 2014. This development provided us with «soft legitimization» of the term «*critical infrastructure*»: while not having the term defined in national legislation we had it in an important official document outlining our country's cooperation with the Alliance.

Another important result of this step was strengthening our relationships with the PDP that provided expert, financial and organizational support to our efforts to develop the GP. Such a support was very important for us since our work in this direction was being placed against the background of the dramatic events in Ukraine resulted in, inter alia, sharp deterioration of the political, economic and financial conditions in the country.

In so doing the agreed with the PDP algorithm of further drafting work was the following:

- Drafting the text of the GP;
- The draft GP circulation among Ukrainian authorities and organizations involved with its simultaneous translation into English for delivering to NATO member-states' experts selected upon the PDP's request to receive feedback;
- Processing comments, notes and proposals received from Ukraine and NATO experts to take their opinions into consideration when developing the next GP version.

To announce the start of GP development and to implement this algorithm the first international expert meeting («kick-off meeting») was convened by the NISS and the PDP on 9 September 2014.

By 15 October 2014 the first version of the draft GP had been prepared by the NISS team and circulated among expert core group members from Ukraine. To provide experts from the NATO member-states with this and later versions of the draft GP it was necessary to translate the document into English.

The next, second, international expert meeting on GP development was carried out on 25 November 2014. Its aim was to track progress and to present the second version of the draft GP in which Ukrainian experts' remarks, notes and proposals were taken into consideration. Besides, this meeting was marked with a very important development for further Ukraine's international cooperation in this field – the representatives of the NATO ENSEC COE took active part in the event and follow-ups.

Final version of the GP was presented on the International Expert Meeting held by NISS and NATO NLO in October 2015[28]. This

[28] International Expert Meeting on the Protection of Critical Infrastructure in Ukraine. – Retrieved from http://www.niss.gov.ua/articles/1960/

document received significant attention, and it was discussed in November 2015 during Ukraine-NATO Joint Working Group on Civil Emergency Planning and Disaster Preparedness meeting in NATO HQ.

At the same time, at this stage of joint efforts a number of methodological and technical difficulties revealed caused by the reasons briefly outlined below.

a) *Novelty of the document (Green Paper) format and CIP concept*. The results of searches in the national databases of legislative and official documents indicated that a GP format, quite a popular in the Western countries, proved to be a rather new one for most of Ukrainian public servants and considerable part of experts. Some of them believe, for instance, that a GP is just another trendy format for documents describing a whole complex of problems existing in a particular field. One more consequence resulted from lack of experience in development and publication of such documents in Ukraine is still the unresolved issue of the GP approval. The question: «Who and how shall approve the GP?» is yet under consideration.

As one of the consequences of poor governance Ukraine suffered for decades, new trends and international developments were often ignored by the authorities including those within the national security sector. That was, in author's view, one of the reasons of this sector degradation, and likely explanation to the concrete fact that the CIP concept proved to be an absolutely new subject matter for most of public servants and experts involved in our efforts.

In combination with lack of a «*critical infrastructure*» definition in the Ukrainian legislation it was resulted in producing proposals aiming at assigning to CI all assets related in one way or another with important functions and services for population and the State regardless of their criticality and time frames within which negative impact caused by their loss might occur. One of the examples of such proposals was a suggestion to include National Parks to the list of CI sectors.

b) *Departmental and institutional interests influence*. It is natural that representatives of authorities, law enforcement bodies, research and other institutions consider a problem in terms of their organizations' missions, responsibilities and interests, but this becomes a problem for development when departmental and institutional interests dominate national ones. In such cases the NISS's experts tried to persuade opponents by means of referring to the experience gained in this field

by the NATO and EU member-states. Nevertheless, the NISS team faced repeatedly departmental interests which revealed themselves in the following forms:

- Intention to maintain the status-quo;
- Aspiration for including a would-be CIP system in existing ones even though they were not capable of addressing all threats and risks by their purposes and missions[29];
- Attempts to re-orient the NISS activities from the very beginning aimed at creation of a national system to protect critical infrastructure towards solely sectoral infrastructures, e.g. energy one.

c) *Technical and organizational problems.* The draft GP developed by the NISS team is a rather large and complicated document. Unfortunately the NISS team failed to fully implement some European experts' recommendations to reduce it to maximum 15 pages. It was already mentioned before that the role of foreign experts in development in drafting has been exclusively important not only due to valuable contribution in a form of notes, comments and proposals, but also because NATO member-states' experts relying upon their countries experience in this field played a role of arbiters when discussions of Ukrainian experts reached a deadlock. But to facilitate their participation in our efforts we *had to provide them with the draft GP versions translated into English.* Ability to communicate in English still remains the problem for a lot of Ukrainian experts and public servants, and the relevant international projects designed to improve this situation remain urgent.

Critical Energy Infrastructure Protection

All countries concerning CIP give without exception the highest priority to their energy sectors among other CI elements. And it is understandable because a modern society is heavily dependent on energy sources practically in all spheres of life. Needs in energy are especially escalated during warfare and armed conflicts leading to critical energy infrastructure (CEI) damage and destruction. Unfortunately, Ukraine has suffered from such negative processes for more than a year being a deliberate target of so called «hybrid warfare».

[29] For instance, the Ukrainian civil protection system does not cover counteraction terrorism, but at the beginning of our effort we had a long discussion with domestic experts who persistently argued to include the CIP into the unified civil protection system.

According to the Information Analysis Center of the National Security and Defense Council of Ukraine[30], as of 17 February 2015 besides the greatest concern emerging from vast number of injuries and deaths caused by «hybrid warfare» it also has led to very severe consequences for infrastructure systems and objects, including those relating to energy supply, namely: 2 772 gas pipelines destroyed; 1 080 energy objects either destructed or damaged; damages and loss of control over the technological processes at the coal mines resulted in reduction in coal mining in Ukraine by 35 %. Under «hybrid warfare» conditions we must pay extraordinary attention to CEI, and Ukrainian experts, like their foreign colleagues, well understand it.

This statement can be confirmed with the development of cooperation between the NATO Energy Security Centre of Excellence and the NISS. It was energy security and CEI protection that were determined as the principal directions of cooperation between the NATO Energy Security Centre and the NISS formally launched on 8 July 2015 in Vilnius with the signing the Letter of Intent on Cooperation by both parties. Particularly, the Ukrainian and NATO experts agreed to cooperate within the framework of the NATO Energy Security Centre's project «Hybrid Warfare and Critical Energy Infrastructure: The Ukrainian Conflict Case-Study» and in other efforts addressing energy security.

Conclusions

The significant progress has been made in introduction critical infrastructure protection concept in Ukraine through drafting the Green Paper on a subject matter which expected to be published October 2015.

Participation of NATO member-states' experts has played a key role in progress achieved providing with relevant expertise and best practice examples.

Efforts aiming at critical energy infrastructure protection shall be considered as those of highest priority and experience gained in this sphere (especially, in nuclear one) shall be disseminated (where applicable) to other sectors of national critical infrastructure.

[30] «Black Book of the Kremlin»: the consequences of Russian aggression in Ukraine were recorded. – Retrieved from http://mediarnbo.org/2015/02/18/chorna-kniga-kremlya-zafiksovano-naslid ki-rosiyskoyi-agresiyi-v-ukrayini/

2.2. CRITICAL INFRASTRUCTURE PROTECTION: THE CHALLENGES OF CONCEPT PRACTICAL IMPLEMENTATION

Ukraine has well-developed state system of physical protection of separated objects of CI. Developing nuclear energy sector Ukraine took obligation to satisfy the international standards on protection of nuclear facilities. Following up international support and internal «historical» legacy of physical protection Ukraine managed to develop a reliable system for physical protection of nuclear facilities and materials that gave an additional push to efforts of developing a new CIP system in Ukraine[31].

However, the system of physical protection of important industrial objects and transport infrastructure was developed for the model of centralized governance and for peacetime. The political and economic reforms in Ukraine (decentralization of decision making), the emergence of new actors and the threats to CI (hybrid threats) have stimulated the changes in this field.

The starting point for the development of a new governmental policy on CIP became development of the Green Paper (GP) on CIP. The final version of the GP was presented by the NISS in October 2015[32] and reflected understanding of the importance of CI stable functionality for national security.

CONCEPT OF A CIP SYSTEM

The GP shapes a CIP system with focus on shifting government and public attention from «reactive» policy removing crisis results to

[31] The system of physical protection system of nuclear facilities and materials is well developed in Ukraine and approved by MAGATE that creates possibility to transfer knowledge and best practice on other types of CI.

[32] International Expert Meeting on the Protection of Critical Infrastructure in Ukraine. – Retrieved from http://www.niss.gov.ua/articles/1960/

crisis's prevention and contingency planning, strengthening coordination of different actors involved and establishing effective PPP relations in the field.

Shortly, eight important points are fixed by GP:

1. Introducing term «critical infrastructure» into the legislation. Currently, the absence of the term leads to confusion in the list of CI assets to be protected what creates difficulties in the effective coordination of efforts between different ministries and agencies.

2. Defining the purpose of a CIP system, namely «to ensure a stable functioning of infrastructure» and by this to guarantee supply of goods and services vital to the population, society, business and government.

3. Shifting the emphasis from the currently dominating dimension of physical protection of systems and facilities to enhancing resilience of CI.

4. Specifying the categories of threats according to the «all hazard approach» (natural disasters, emergencies and technical failures, malicious activities) focusing on elements of CI that could be targeted (physical elements, management and communication systems, facilities, personnel).

5. Fixing trilateral goal of a state CIP system that, namely to ensure:

a) smooth functioning of CI (reliability);

b) ability to resist against the threats (resistibility);

c) ability to recover operations in case of interruption within a certain time period (resilience).

All these aspects should be reflected in contingency planning of CI operators as well.

6. Establishing government approved criteria to assign certain facilities and systems to list of CI[33].

7. Predefining:

- operational regimes of CI (procedures) and modes of control of a CIP system (both at a state and CI operator levels);
- related organizational, institutional, economic and law regimes of CI facilities functioning in accordance with levels of threats.

[33] The GP considers following characteristics as a factors to be taken into consideration to assess criticality of CI objects: scale of influence; infrastructure connectivity; time of occurring; object vulnerability; consequences severity (economic loses, internal and state security, psychological, safety of life, defense capacity, environmental safety).

8. Designing institutional and organizational structure and responsibilities of the involved parties.

We suggest using four operational modes of CI functioning and CIP system's regimes:

«Green» – early warning (threat anticipation and prevention) – normal mode of CI functioning; normal legal and economic regimes. A CIP system works on anticipation and prevention of threats, utilizes an early warning tools;

«Yellow» – alert (threat determent and CI protection) – normal mode of CI functioning; normal legal and economic regimes. In case of threat identification, a CIP system switches to early warning regime of CI functioning. A CIP system works for protection of selected facilities within designed object protection system (internal resources), checks on preparedness of external resources in order to prevent threat realization;

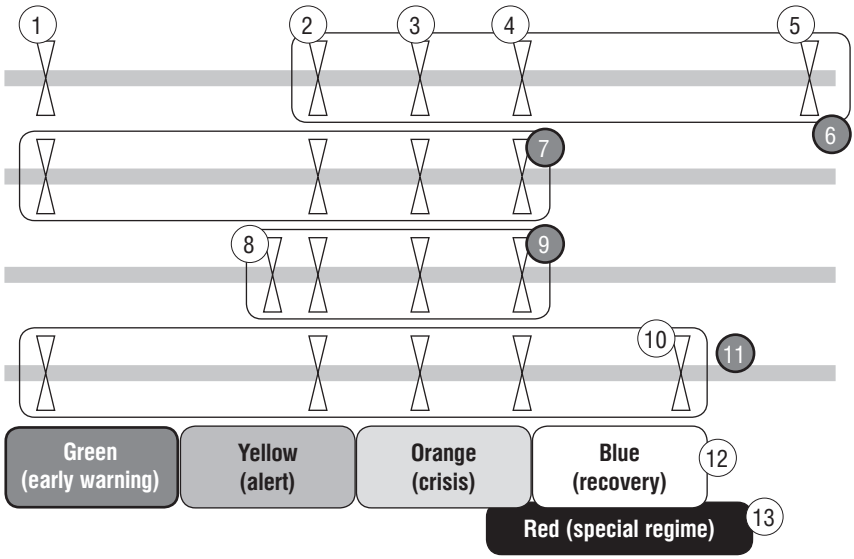
«Orange» (***threat suppression and CI disruption mitigation***) – special mode of CI functioning, some restrictions in legal and economy regimes (similar regimes on power market have been introduced in Ukraine few times in 2014–2017 years). A CIP system works for suppression of threats and mitigation of negative impact on CI functioning. A CIP system utilizes needed external forces and resources to eliminate threats and negative consequences;

«Blue» – (***threat response and CI functioning recovery***) – special mode of CI functioning; serious restrictions in legal and economy regimes. A CIP system works for recovering ability of CI perform its functions for society and state;

«Red» (***threat response***) – special mode of CI functioning; serious restrictions in legal and economy regimes; state could take full control over regime of CI functioning. A CIP system utilizes all available forces and resources within special period[34] (legal framework) of governance (war, emergency).

Explanation of proposed approach for a CIP system design together and comparison of responsibility of available in Ukraine systems is given on *Fig. 2.2.1*.

[34] Special period means period when state of «war» or «national level emergency» is officially declared.



1. Threat analysis
2. Risk assessment
3. Emergency at an object
4. Ending of emergency at an object
5. Consequences elimination
6. Civil protection system (protection of population)
7. Counterterrorist system (protection of military and state objects)
8. Vulnerability evaluation
9. Physical protection system (protection of nuclear facilities)
10. Recovery of functions
11. CIP system (to provide reliability, resistibility and resilience of CI)
12. Modes of CIP system operation
13. Period of war

Fig. 2.2.1. **The CIP system's domain of responsibility**

CHALLENGES OF A CIP SYSTEM INTRODUCTION

The planned pace of GP development and practical implementation of its provisions were accelerated due to «hybrid war» against Ukraine. The «Green Paper» project, starting as scientific research activity, was transformed into practical task to launch new security policy of Ukraine. In addition, new tools of warfare stipulated the need to reassess the paradigm of CIP, shifting attention from «protection» to «resilience» of

CI[35]. As well, there was emphasized that buildup of CIP state system has to be aimed at enhancing resilience of the infrastructure against hazards of any kind.

This situation created challenge of capability and acceptance of the initiative. Any change in existing systems, setting new set of tasks and goals is very challenging task for every country, but for Ukraine in times of war it became extremely difficult. There was the need to create a «critical mass» of support for new concept in government agencies and ministries as well as capability of staff to accomplish established tasks in limited timeframe, emergency, lack of resources and knowledge in the field of activity.

Another challenge that required attention was the need to specify the role/place of the CIP concept within the national security domain as well as tasks and duties of involved actors. Existed state systems which covered some areas of CIP demonstrated some resistance to fast changes.

Currently in Ukraine it is hardly possible totally change existing institutional structure of involved agencies in the CIP domain. Therefore, GP proposes to differentiate events related to CI malfunctioning according to main duties of the existed systems. It could create possibility of combining efforts of different systems by developing procedures of IEI. It is important to combine efforts of the most relevant systems that have been established in Ukraine earlier: the civil protection system – ISSCP; the physical protection system – SPPS; the counter-terrorism system – USSPRM-T; the cyber security system – NCSS (started to develop in 2016 year).

One of the priority tasks of CIP system development in a near future is to clarify procedures of interagency interaction and exchange information (IEI) taking into account existence of competition for «influence» in the current structure of governmental bodies. So, «unintended events» like technical errors, accidents, natural disaster, etc. could be managed with the help of existing civil protection system while «targeted (malicious) actions» require the development of «prediction» and use of tools to respond to terrorist treats by the relevant counter-terror system.

From the formal point of view, the adoption of such approach partially solves the problem of coordination in the field of CIP, especially

[35] Sukhodolia O. Protection of critical infrastructure in hybrid warfare: problems and priorities of state policy of Ukraine // Strategic Priorities. – 2016. – 3. – P. 62–76

in the cases of emergency. However, it is impossible to establish a comprehensive CIP system totally based on existing systems, like the existing system of civil protection or counter-terror systems. There have to be entity that would develop and operate procedures of interagency interaction and exchange information on CIP.

The NISS analysis indicated that the best organizational approach consists of establishment of *national center for crisis management and critical infrastructure protection* (NCCM&CIP) which has to be tasked with informational, analytical and methodological support of a CIP system and combining efforts of the existed system through national and sectorial situational centers as a part of the national network of distributed situational centers (crisis centers within different systems). The added value of a CIP system is to present institutional basis for «preventive and contingency planning» to secure CI stable functionality and resilience.

The urgency of the issue and awareness of the CIP system problems became supportive by achieving general understanding of further actions in this field. The CIP became one of the priorities of newly adopted National Security Strategy of Ukraine, which introduced priorities of further activity at the issue[36].

Further there were adopted other legislation acts of strategic importance, which tasked different government agencies and ministries on CIP. The most important of such acts were NSDCU decisions that introduced:

- Concept of further development of Security and Defense sector of Ukraine[37];
- Cyber Security Strategy of Ukraine[38];
- Measures on providing critical infrastructure protection[39];

---

[36] Decree of President of Ukraine of 26 May 2015 № 287/2015 «On National Security Strategy of Ukraine». – Retrieved from http://zakon3.rada.gov.ua/laws/show/287/2015

[37] Decree of President of Ukraine of 14 March 2016 № 92/2016 «Concept of further development of Security and Defense sector of Ukraine». – Retrieved from http://zakon2.rada.gov.ua/laws/show/92/2016/paran2#n2

[38] Decree of President of Ukraine of 15 March 2016 № 96/2016 «On Cyber Security Strategy of Ukraine». – Retrieved from http://zakon2.rada.gov.ua/laws/96/2016

[39] Decree of President of Ukraine of 16 January 2017 № 8/2017 «On improvement of the measures to ensure protection of critical infrastructure objects». – Retrieved from http://zakon2.rada.gov.ua/laws/8/2017

- Measures to neutralize energy security threats and to strengthen critical infrastructure protection[40].

The mentioned acts became the legal foundation for further development of a state the CIP system. The NSDCU decision «On the improvement of measures on providing critical infrastructure protection» tasked Cabinet Ministers of Ukraine together with Security Service of Ukraine (SSU) and the NISS to develop «Concept for building a state critical infrastructure protection system in Ukraine» and the draft Law of Ukraine «On critical infrastructure and its protection».

In fact, at present there is consensus on the need to implement contingency planning and risk management concept into Ukrainian legislation and practice of governance with the aim to prevent interruption of CI functioning.

The SSU took a leading role in CIP concept implementation. In accordance with priorities of reform of Security and Defense Sector of Ukraine within SSU was created special department on CIP that was tasked to provide threat identification, intelligence informational exchange and coordination of efforts of government agencies on some aspects of CIP[41].

In the summer of 2017, SSU and Ministry of Economic Development and Trade of Ukraine established inter-ministerial working groups to prepare needed draft of legal acts required by the NSDCU decision.

By the end of 2017 in order to develop the methodology for assigning infrastructure objects to critical energy infrastructure and to prepare recommendations on procedures of such objects passportization and categorization the interagency working group was also established under the Ministry works on establishment of Energy Crisis Center that have to become a tool for information exchange between all involved agencies responsible for stable and resilient functioning of energy sector of Ukraine[42].

---

[40] Decree of President of Ukraine of 16 February 2017 № 37/2017 «About On urgent measures on neutral ization of energy security threats and strengthening of critical infrastructure protection».– Retrieved from http://www.president.gov.ua/documents/372017–21302

[41] Sukhodolia O. Critical infrastructure protection: modern challenges and priority tasks of security sector // Scientific Journal the Academy of National Security. – 2017. № 1–2. – P. 50–80.

[42] The Order of Ministry of Energy and Coal Industry of Ukraine of 20 Luly № 37/2017 «On establishment working group on assigning infrastructure objects to critical infra structure».

Other ministries mentioned in GP as responsible for sectors of CI started paying attention to their area of responsibility as well.

All above mentioned activity revealed another challenge to the process of CIP implementation, specifically overcoming habitual routine and traditional procedures from government bodies as well as operators of CI, namely:

- changing habitual practice of involved actors' activity;
- developing of new tools and their application under time and resource constraints;
- getting new knowledge and skills;
- ensuring mutually supporting actions of all involved actors (state, public, industry).

The NISS, in order to find a way to resolve the problem launched decrease a set of raising awareness, education and training events (for practical example of training see chapter 2.4).

FURTHER DEVELOPMENT OF THE CIP SYSTEM

The set of main tools of the CIP system is already partly in place in Ukraine. The following tools could be adapted to a CIP system: «Design basis threat»[43], «Preventive Action Plan», «Emergency Plan», «Communication System (IEI)», «and Training».

The «Design basis threat» for nuclear and radioactive materials and related facilities («Projected threat» in Ukrainian legislation) was approved by NSDCU in 2009 and later updated to develop «Object projected threat» for objects assigned to the government approved list.

The «Preventive Action Plan» on CIP developed by operators, agreed and approved by the relevant governmental authorities as well as «National Preventive Action Plan» must contain the detailed description of measures to identify and mitigate threats in different areas.

The «Emergency Plan» on CIP must contain the detailed description of recovery measures in case of crisis. The practice of emergency planning is well developed in Ukraine, especially in the civil protection system. There should be improvements to address issues of

[43] The «Design basis threat» – the attributes and characteristics of potential insider and/or external adversaries, who might attempt unauthorized removal or sabotage, against which a physical protection system is designed and evaluated (MAGATE-INFCIRC/225/Revision 5).

interconnectivity and interchangeability of CI as well as changes in CI functioning regimes.

The «Communication system» (information exchange, efforts coordination) is well developed in a framework of physical protection of nuclear facilities. Proposed communication procedures contain certain formal elements on different levels of responsibility. Among important elements of the communication system there should be plan of interaction of central and local authorities on physical protection that requires:

- Regional plan for actions on physical protection, which regulates the involvement of military units and other law enforcement agencies of a region;
- Object plan for action on physical protection developed upon requirements of «Object projected threat», which regulates interactions of involved actors on object's level;
- Communication and interaction procedures, which establish requirements for format of interaction of agencies, clarify responsibilities of the agencies involved into acting in accordance with object and regional plans, timing of actions.

The «Training» exercises, which have to be designed to practice staff of involved forces, to improve their skills, to check performance of tools. The goal of training is to ensure the readiness of forces and tools of involved agencies to perform needed actions and procedures.

FINDING SUPPORT FOR THE PROCESS OF CIP CONCEPT

The process of Green Paper on CIP development has helped to identify the elements needed for a successful work:

1. Involve experts from the private sector and state agencies in designing a CIP system. It helps to shape right ideas of the GP as well as create support in order to facilitate «transfer» of new concepts into public entities activity. At the same time, it helps clarify provisions and escape legal traps and create common understanding of future cooperation between institutions.

2. Use existing institutions. Institutional structure which exists today, for example civil protection or counter-terror system could be used for implementation of a new CIP concept. However, the focus of the activity should be tuned. Countering malicious acts, like acts of

sabotage, could be resolved by means of the counter-terror system. However, CIP should cover also other types of targeted actions that include political decisions of other states too (like a decision of Russia to halt energy supply to Ukraine). Ensuring continuity of functions infrastructure provides is not a protection of habitual conditions of citizens' life what supposed to remain the domain of civil protection service.

3. Engage existing tools. Some threats to the stable functioning of CI could be generated by malicious actions, but the big part of threat is generated by technical errors, accidents, natural disaster etc. In general, a CIP system should be capable to propose two-level package of measures, namely measures aimed at threats diminishing and crisis resolving. The goal of a CIP system is to minimize the risks of ending of operation of CI through building tools of protection (priority for reliability and resistibility) as well as to prepare options for quick restoration of CI functionality (priority for resilience).

4. Demonstrate added value of a CIP system. The growing threats from malicious actions against CI require a proactive policy. A CIP system will assess the risks to continuity of infrastructure functions through cooperation of government as well as operators of CEI through establishing close private-public partnership decreasing state expenditures.

That target requires the establishment of «preventive action planning» giving special attention not only to build physical protection at all stages of life cycle of CI (design, location, construction, installation, commissioning, operation and liquidation of consequences) but also to develop interconnectivity of CI, availability of needed reserves, involvement of private sector resources.

5. Utilize best practice. International experience and support is very important, especially for countries that are limited in time and resources to develop a CIP system on its own. It is important not only through using «best practices», methodology or legislation but also through direct involvement of experts in development pieces of legislation.

For example, concerning energy sector of Ukraine in 2015 the elements of «contingency planning» were developed by the team of experts from USA, Canada and EU countries and implemented into draft of «Plan for functioning of Energy Sector of Ukraine in winter period of 2015/2016» and «Plan for achieving of energy sustainability of Ukraine».

Other relevant examples of international cooperation within CIP concept development includes:

- development of conceptual policy papers on CI and development of framework legislation. The GP on CIP has been created by the NISS with the active support of experts from NATO countries;
- education of staff of ministries and agencies involved in CIP system functioning. The NATO PDP has vastly contributed and supported the NISS in organizing series of seminars on CIP in 2013–2015 years;
- training the staff of ministries and agencies. So, the NISS and the NATO Energy Security Centre of Excellence organized Table Top Exercise on Critical Energy Infrastructure Protection, which was held in Ukraine in October 2017.

2.3. THE PROBLEMS OF DIFFERENT STATE SYSTEMS INTERACTION: IMPLICATION FOR ENERGY SECTOR

There is no single response or protection system that would be available to respond to all types of crisis situations. Different types of crises trigger different crisis prevention and response systems and, accordingly, require involvement of different entities.

At present, as was mentioned before in Ukraine have been established following response and protection systems that cover some aspects in CIP:

- The Unified State System for Civil Protection (USSCP);
- The Unified State System for prevention of, responding to and suppressing terrorist acts and mitigation their consequences (USSPRM-T);
- The State Physical Protection System (SPPS);
- The National Cyber Security System (NCSS).

The analysis of existing systems of emergency response and protection allows making some conclusions that determine the task of improving of the existing systems on prevention and response to crisis situations.

First of all, it should be noted the differences in the orientation of existing state systems. The most elaborated, both in terms of the legal framework and of practical implementation, there are three systems:

1. **The Unified State System for Civil Protection (USSCP)** directs the efforts of the all subjects of the system, subordinated forces and means for actions aimed at preventing and responding the emergency situation and focuses on protecting the population and territories from consequences of emergency situation.

The system is multi-level (includes state, regional, local level and the levels of facilities) and consists of permanently operating functional and

territorial subsystems. The coordination of the USSCP activity is realizing by the State Extraordinary Commission.

The functional subsystems of the USSCP are creating in the relevant spheres of social life by central executive authorities aiming to protect the population and territories in case of emergency situations in peacetime and during the special period, to ensure the preparedness of subordinated forces and means for actions directed to prevent and response on emergencies. The direct management of such functioning subsystem is provided by the head of the body or entity that created this subsystem.

The territorial subsystems are creating in regions with the aim to implement measures to protect the population and territories in the relevant regions. The direct management of such territorial subsystem is provided by the officials who are a head of the body or entity that created this subsystem.

The general regulations on functional and territorial subsystems of USSCP are approved by the resolutions of the Cabinet of Ministers of Ukraine (CMU) and acts of SESU.

2. **The Unified State System for prevention of, responding to and suppressing terrorist acts and mitigation their consequences (USSPRM-T)** is aimed on prevention terrorist activities, including providing timely identification and elimination the causes and conditions that facilitate committing the terrorist acts.

The system consists of permanent territorial and functional subsystems: the coordinating groups of the Counter-Terrorism Center (CTC) of the Security Service of Ukraine (SSU) at the regional SSU's units and their headquarters (territorial subsystem); and the structural units of the subjects combating terrorism and the Interagency Coordinating Commission of the CTC SSU (functional subsystem). These subsystems interact by sharing information about the threat to commit a terrorist act, monitoring the status and trends in the spread of terrorism in Ukraine and over the world, organizing and conducting the joint rescue operations and other activities, by conducting command-staff and tactical-special exercising and training with the use of forces and means of the subjects fighting terrorism.

3. **The State Physical Protection System (SPPS)** is aimed on protection, prevention and suppression of sabotage, theft or any other illegal extraction of nuclear material, radioactive waste and other sources

of ionizing radiation, as well as on the strengthening the nuclear non-proliferation regime.

The procedure of the functioning of this system is approved by the resolution of the CMU and SNRIU. This procedure determines the principles of the state system functioning only regarding physical protection for the selected nuclear installations and nuclear materials, radioactive waste, and sources of ionizing radiation.

All these systems have well developed mechanisms of interaction between involved subjects (vertical and horizontal level) as well as the developed and tested in practice plans of interaction.

In all of these systems the ministries that are responsible for stable functioning of certain CI sectors have to play a certain role described legal acts as of national level (laws, orders of CMU and President of Ukraine) and ministerial or territorial level.

For example the Ministry of Energy and Coal Industry of Ukraine (MoECI), as a central executive authority, which forms and implements the state policy in the energy sector, has to be coordinator of actions regarding critical energy infrastructure.

Within the USSCP namely MoECI is responsible authority for ensuring the operation of the functional subsystems "Security Subsystem of electricity and nuclear-industrial complex", "Subsystem on Security of Oil and Gas complex" and "Subsystem on Security of the coal industrial complex". In frame of the USSPRMT the MoECI is responsible authority for ensuring operation of the Ministerial Functioning Subsystem. Within the SPPS the MoECI provides the implementation of the state policy on physical protection of the system's objects at the subordinated enterprises.

CORRELATION OF OPERATION REGIMES OF DIFFERENT STATE SYSTEMS OF EMERGENCY RESPONSE AND PROTECTION

Each of the described above state systems (USSCP, SPPS, ISPRM-T) has its own regimes of functioning specified by legislation of these systems.

Depending on the security and safety conditions, the scale and nature of an emergency either foreseen or emerged, one of the next regimes of the USSCP is established throughout the country or within its concrete region:

- the everyday functioning;
- the high level of preparedness;

- the emergency situation;
- the emergency state.

The list of measures, which are provided under relevant regime, the tasks and the order of the interaction of the subjects ensuring the civil protection, are determined by the Provision on the USSCP.

In the normal conditions of economical, radiation, chemical, seismic, hydrogeological, hydrometeorological, man-caused and fire situation and in case of the absence of epidemics, epizootics, epiphytotic the USSCP is functioning in the routine (everyday functioning) regime.

The basis for the introduction (activating) of the regime of the high level of preparedness on the relevant level is the threat of the emergency appearance, for the introduction of the regime of the emergency situation – is the occurrence of the emergency of the relevant level. The level of emergency is determined in accordance with the Classification of the emergency situations.

The regime of the high level of preparedness and the regime of the emergency situation in Ukraine or within its concrete territory are introduced:

- on the territory of the whole state or its separate regions – by the decision of the CMU;
- on the territory of the relevant region – by the decision of the Council of Ministers of Autonomous Republic of Crimea, regional (oblast) state administrations, Kyiv and Sevastopol cities state administrations;
- on the territory of the relevant district (city, town) – by the decision of the district state administration and local governments.

In case of the introduction of the emergency state, the USSCP acts as it is foreseen in the Code of Civil Protection and taking into account the peculiarities determined by the Law of Ukraine *On the legal regime of the emergency state*.

The State system to combat terrorism (USSPRM-T). Depending on the available information about the threat or in the case of a terrorist act there are following levels of terrorist threats:

- «grey» (possible threat) – in the presence of factors (conditions) facilitating the commission of terrorist act;
- «blue» (potential threat) – if the information requires the confirmation of the preparation to commit a terrorist act;
- «yellow» (likely threat) – in the presence of reliable (verified) information about the preparation to commit a terrorist act;

- «red» (real threat) – in case of terrorist act.

The level of terrorist threat temporarily introduced for all or separate subjects combating terrorism and acts on the whole territory of Ukraine, or in certain its areas or at the facilities of the possible terrorist attacks.

The decision on the introduction, modification, cancellation of the terrorist threat level, the period and area of the action of the relevant level of terrorist threat is made by the head of the CTC SSU with the written permission of the Head of the SSU. The head of the CTC immediately informs the President of Ukraine about such decision. The decision itself is made public through the mass media.

The state system of physical protection (SPPS) operates in such conditions:

- the normal functioning;
- the increased readiness;
- the functioning in the crisis situation;
- the restoration of the normal functioning.

The decision to change the conditions of the state system of physical protection functioning is adopted by the SNRIU on the basis of the submitted information by the subjects of the system and other bodies. The SNRIU informs the subjects of the system about the changes in the conditions of their functioning.

The conditions for the normal functioning are valid in case of the absence of reliable information about the threat of sabotage, theft or any other illegal extraction of radioactive materials.

The decision about the SPPS functioning in the conditions of the increased readiness is adopted if the reliable information about possibility of sabotage, theft or any other illegal extraction of radioactive materials at the objects of the system is available within the SNRIU.

The decision about the SPPS functioning in the conditions of the crisis situation is adopted in case of sabotage, theft or any other illegal extraction of radioactive materials at the objects of the system, which led to the inappropriate radiation consequences.

So, it should be noted that each of the state systems reviewed above (USSCP, SPPS, USSPRM-T) has its own range of operational regimes defined in regulations on these systems. At the same time, generic operation regimes could be derived based on appropriate threat levels (see *Table 2.3.1*).

Table 2.3.1. **Correlation of Operation Regimes of USSCP, SPPS and USSPRM-T**

System/ Regime	USSCP	USSPRM-T	SPPS	Generic Regime
	everyday operation regime	«gray» and «blue» levels of terrorist threat	normal operation	normal operation
	high readiness regime	«yellow» level of terrorist threat	the increased readiness	high alert
	regime of emergency situation	«red» level of terrorist threat	crisis operation	crisis operation
	regime of emergency state		recovery to normal operation	

Note: at present (September 2017), regimes of functioning of the National Cyber Security System (NCSS) still is not identified in legislation.

Note that different systems engage different actors in the prevention of and response to crisis situations in different operational regimes.

Comparative analysis of actors involved in response to crisis situations under existing systems is provided in *Table 2.3.2.*

Table 2.3.2. **List of Principal Actors Involved in Response to Crisis Situations within the Existing Systems**

The list of subjects/ Systems	USSCP	SPPS	ISS PRM-T	NCCS
Security Service of Ukraine (SSU)		+	Main	+
Ministry of Internal Affairs of Ukraine (MIA)	+	+	+	
National Police of Ukraine (NPU)	+		+	+
National Guard of Ukraine (NGU)		+		
Foreign Intelligence Service of Ukraine (FIS)		+	+	+

The list of subjects/ Systems	USSCP	SPPS	ISS PRM-T	NCCS
State Emergency Service of Ukraine (SESU)	Main	+	+	
Ministry of Foreign Affairs of Ukraine (MFA)		+	+	
State Nuclear Regulatory Inspectorate of Ukraine (SNRIU)	+	Main		
State Nuclear Regulatory Inspectorate (regional subsidiaries)		+	+	
Ministry of Energy and Coal Industry of Ukraine (MoECI)	+	+	+	
Ministry of Infrastructure of Ukraine (MoI)	+		+	
Ministry of Envitonment and Natural Resources of Ukraine (MoE)	+		+	
State Hydrometeorological Service	+		+	
State Agency of Ukraine on Exclusion Zone Management		+	+	
State Agency for Forest Resources of Ukraine				
State Agency of Water Resources of Ukraine				
State Geological Service of Ukraine				
Ministry of Economic Development and Trade of Ukraine	+		+	
Ministry of Agrarian Policy and Food of Ukraine	+		+	
Ministry for Regional Development, Building and Housing of Ukraine	+			
Ministry of Health of Ukraine (MoH)	+		+	
Ministry of Defense of Ukraine (MoD)	+	+	+	+

The list of subjects/ Systems	**USSCP**	**SPPS**	**ISS PRM-T**	**NCCS**
The General Staff of the Armed Forces of Ukraine (AFU)	+	+	+	+
The Main Intelligence Department at the Ministry of Defense of Ukraine				+
State Service of Special Communications and Information Protection of Ukraine (SSSCIP)			+	Main
State Border Guard Service of Ukraine (SBGS)			+	
State Service of Ukraine on Export Control			+	+
National Academy of Sciences of Ukraine		+	+	
Regional executive authorities		+	+	
Local executive authorities		+	+	
Non-government organizations	+			
Security Service of Ukraine (SSU)		+	Main	+
Coordinating centers / Systems	**USSCP**	**SPPS**	**ISS PRM-T**	**NCCS**
President of Ukraine				
Government of Ukraine	+			
National Security and Defense Council of Ukraine, National Coordination Center for Cyber Security at NSDCU				+
Security Service of Ukraine (SSU)		+		
State Nuclear Regulatory Inspectorate of Ukraine (SNRIU)				
Interagency Operations Headquarters (IOH at the MoECI)		+		
Regional executive authorities	+	+		
Local executive authorities	+	+		

The list of subjects/ Systems	USSCP	SPPS	ISS PRM-T	NCCS
Special commissions on emergency situations response and liquidation of their consequences (at state, regional and local levels)	+			
State Service of Special Communications and Information Protection of Ukraine (SSSCIP)				+
President of Ukraine				
Situation and Crisis Centers	**USSCP**	**SPPS**	**ISS PRM-T**	**NCCS**
Counter-Terrorism Center at the Security Service of Ukraine (CTC SSU)			Main	
State Emergency Management Center at the State Emergency Service of Ukraine (SEMC SESU)	Main			
Information and Crisis Center of the SNRIU (ICC SNRIU)		Main		
Crisis Centers of the licensees				
State Center for Cyber Protection and Cyber Threat Suppression (SCCP SSSCIP)				Main
Suggested Sectoral Situation and Crisis Center of the Ministry of Energy and Coal Industry of Ukraine	Interaction / Main (at object)	Main / Interaction (inside facilities)	Main (at the branch level) / Interaction	Informing
Managerial staff, headquarters (IOHs)	+			

Note: «Main» – the chief authority; «+» – participant of system.

It should be emphasized that the USSCP is mostly directed toward elimination of crisis consequences, thus any activities of system actors should be initiated after the crisis occurrence.

However, for example in energy sector, the functional capability of the power sector infrastructure (its ability to provide services) in the current environment could be warranted by resilience of Ukraine's energy sector to the threats, which means, inter alia, prevention of crisis situations. Thus in fact, the focus of the crisis response system

needs to be shifted from elimination of consequences toward crisis prevention.

There are generally two systems designed to achieve this task: physical protection system – SPPS and system to combat terrorism – USSPRM-T.

These systems, while having related goals, are guided by different agencies, are largely uncoordinated and partly compete with each other. They are built to respond to different basic concepts, which at the end affect the coordination and information exchange mechanism. They also use different terminology, which further defines the mechanisms of interaction and information exchange. For example, terms 'sabotage' (the SPPS) and 'terrorist acts' (the USSPRM-T) have different meaning.

SPPS guides its actors "to protect interests of the national security, prevent and interrupt sabotage, theft or any other unauthorized removal of nuclear material, radioactive waste, and other sources of ionizing radiation and to enhance nuclear non-proliferation regime." In fact, this sense of 'sabotage'[44] makes the SPPS focus primarily to keep nuclear or radioactive materials at their designated locations.

In its turn, the USSPRM-T is aimed for the prevention of, response to and suppression of terrorist acts as well as for the minimization of their consequences[45].

Terrorist acts are construed as "*criminal acts involving use of weapons, explosion, arson or any other act punishable under Article 258 of the Criminal Code of Ukraine*."

In its turn, the Criminal Code of Ukraine clarifies that a '*terrorist act*' is an *act that causes disruption of public order or detriment to*

[44] In the Law of Ukraine *On Physical Protection…*, «**sabotage** means any deliberate act of an individual or a group of individuals directed against nuclear facilities, nuclear material, other sources of ionizing radiation in use, storage or transport or against radioactive waste being handled, which could directly or indirectly endanger health and safety of personnel, the public or the environment by exposure to ionizing radiation or release of radioactive substances,» whereas «the operation of the State Physical Protection System **is based on results of threat assessment in respect of sabotage**, theft or any other unauthorized removal of radioactive material».

[45] In the Law of Ukraine «On Combating Terrorism» the terrorism «means socially dangerous activity involving conscious and purposeful use of violence including the taking of hostages, arson, murder, torture, intimidation of the public or government authorities or other encroachments on life or health of innocent people or threats to commit crime to achieve criminal purposes».

human health, while 'sabotage' involves acts aimed for the impairment of the state[46].

Because of these legal inconsistencies the focus of the SPPS on interruption of sabotage (limited to nuclear and radioactive materials) leaves the USSPRM-T inactive in certain cases. For instance, some practical issues, such as protection of Nuclear Power Plans (NPP) site equipment from damage that would not cause "exposure to ionizing radiation or release of radioactive substances" or equipment outside the NPP site whose damage may gravely affect NPP operation, remain unregulated.

From the formal standpoint, two concepts of malicious activities, 'terrorist acts' and 'sabotage', used in the legal framework, only confuse crisis response. While the best security practice is to enhance coordination between different security systems, up to their full integration (which follows from broad acceptance and implementation of the all hazards approach), terminological confusion in respect of concepts used to define identical sets of tasks leads to the domination of narrow departmental approaches and preservation of interagency barriers.

STATE RESPONSE AND INTERACTION PLAN IN THE EVENT OF SABOTAGE ON NUCLEAR FACILITIES

Ukrainian legislation provides example of efforts to create a coordination of efforts of different actors in the field of protection. «The State plan of interaction between central and local authorities in case of

[46] In the Criminal Code of Ukraine the term sabotage means «commitment, for the purpose of impairment of the state, of explosions, arson, or other acts aimed for the mass killing of people or causing injuries or health detriments, destruction of or detriment to facilities critical for economy or defense, and commitment, for the same purposes, of acts aimed for radioactive contamination, mass poisoning, spread of epidemics, epizootics or epiphytotics;» while terrorist act means «use of weapons, explosion, arson or other acts that endanger human life or health or cause substantial economic detriment or other severe consequences, where such acts are committed to disrupt public order, intimidate the public, provoke a military conflict or international tensions or to influence a decision of a government authority, local governing body, their officers, public associations or legal entities to act or withhold from action, or to attract public attention to certain political, religious or other views of the perpetrator (terrorist), as well as a threat to commit the said acts for the same purpose».

committing sabotage on nuclear facilities, nuclear materials and other sources of ionizing radiation during their use, storage or transportation, as well as radioactive waste in the process of management with them» (State Response and Interaction Plan – SRIP) was approved by the Resolution of the CMU from 24 July 2013, № 598[47].

It determines the procedures and mechanisms of interaction between the state authorities and other entities in response process. SRIP is a practical coordination tool for all participants of SPPS (as well as USSCP and USSPRM-T) and prescribe to establish interagency headquarters within MoECI to provide interaction and exchange of information in case of crisis.

In practice there is a ground for improvement. Practical assessments of the SRIP reflect key observations:

1) SRIP defines the goal of coordination between SPPS participants, which includes description of key legal and administrative aspects of coordination between central and local executive authorities, National Academy of Sciences and SSU within the SPPS framework, as provided in the Law of Ukraine *On Physical Protection…*[48]

Unfortunately, this part of the Law, passed back in 2000, has become obsolete and does not reflect current processes and approaches in the area of nuclear terrorism suppression (nuclear security) seeing physical protection as just one (although major) element of nuclear security. Obviously, the broader scope of tasks related to nuclear and radiological terrorism suppression should be implemented by a larger number of actors involved in response to malicious acts against nuclear facilities and nuclear material.

2) SRIP gives a partial answer to modern challenges by assuming deployment of MoD personnel and equipment in case of "particularly severe man-induced or natural emergency situations" – this was not

[47] Resolution of the CMU of 24 July 2013 № 598 «On approval of the state plan of interaction of the central and local executive bodies in case of sabotage on nuclear installations, nuclear materials, other sources of ionizing radiation in the process of their use, storage and transportation, as well as in the process of radioactive waste management». – Retrieved from http://zakon3.rada.gov.ua/laws/show/598-2013-%D0%BF

[48] Law of Ukraine of 19 October 2000 № 2064-III «On physical protection of nuclear installations, nuclear materials, radioactive waste, other sources of ionizing radiation». – Retrieved from http://zakon4.rada.gov.ua/laws/show/2064-14

provided for either of the USSCP or the SPPS. On the other hand, this option is only limited to crisis situations that are beyond the DBT.

NPP protection is designed based on a facility-level DBT based on the specific regional situation and referring to issues specific to the particular NPP. Neither the facility-level design basis threat, nor the national DBT dwells on potential actions of a military component or the impact of the domestic political situation (or situations in neighbor states) on the level of threat or the coordination in case of a crisis situation.

No consideration is given to local communities as a potential threat to NPPs. This view rests on the assumption that residents of territories adjacent to an NPP depend on the plant (many of them work at the NPP or enjoy discounts from electricity or heat supply tariffs). The same concerns peaceful protests only because they have not taken place in the past.

Although no rallies are allowed in the NPP control areas by applicable laws, the experience of the hybrid war of Russia against Ukraine shows that peaceful protests may be used as a cover for criminal activity. Specific attention should be paid to potential provocations aimed to demonstrate that Ukraine is unable to protect its nuclear power plants.

The threats described above may turn to be outside the scope of the SRIP; thus response plan participants will be under no obligation to cooperate and participate in exchange of information and coordination system. Therefore it is expedient to broaden a circle of parties involved in coordination, in accordance with the all hazard approach.

3) As regards coordination procedure, it should be noted that this key section of the SRIP has not been tested practically. The procedure of interaction and exchange information itself is not clearly aligned with the existing state systems and does not regulate information exchange, including from the standpoint of operation regimes of various systems. Plan proposes participants to maintain communication and exchange information "*on existing potential threats to such extent as would be sufficient to make decisions on appropriate actions…*".

Firstly, it is doubtful that coordinating parties will be able to maintain such exchange under pressure of an emergency situation without appropriate regulations (covering content, scope and format of information exchange) developed in advance. Particularly this

concerns the requirement to notify chief executives of SRIP participants "in a threat of sabotage against a nuclear installation or nuclear material…". SRIP does not specify who exactly should be responsible for such notification.

Secondly, the requirement to establish an 'interagency operations headquarters' is not consistent with the legal requirements for the activation of existing systems already having their crisis centers and headquarters.

Thirdly, the provision concerning minimization of sabotage consequences focuses on radiological consequences only, which again is not consistent with modern approaches whereby capabilities should be in place to respond to all types of threats, as well as to combined threats.

4) As regards authority of its participants, the SRIP does not provide clear understanding of tasks and authorities of certain participants that are not covered by mechanisms within existing systems.

It is unclear, what agency is directly responsible for neutralization of terrorists encroaching on nuclear fuel or nuclear materials and how this agrees with the authority of MIA and SSU.

Work with the public is limited to notification in case of sabotage and communication of a radiological situation (both the responsibility of local authorities).

Under a combined threat, such notification and communication in a crisis situation will require involvement of not only the State Emergency Service of Ukraine, but also, in the least, the SSU.

5) Top political component is left altogether outside the framework, although escalation of a conflict will require political decisions.

6) Considering the all hazard approach it makes sense to expand the number of SRIP participants by adding a number of other government agencies, organizations and companies.

The list of actors to be involved in SRIP implementation may vary depending on the identified type of threat (crisis) and the state response and protection systems activated.

7) It makes sense to establish a first response unit within the framework of one of the crisis response actors whose task will be the initial identification of the crisis type. Personnel of such a unit should be prepared to respond to chemical, biological, radiological and nuclear threats and terrorist threats.

8) MoD and Armed Forces of Ukraine (AFU) should be allowed to play a more active role in the response to crisis situations, since escalation of a crisis may threaten national security as well as broader regional and global security. A special working group should be established to work out proposals on the format, procedure and protocols for exchange of information.

9) Since acts of terrorism (sabotage) against critical infrastructure like nuclear facilities or nuclear material may have global consequences and threaten national security, clear mechanisms should be established within framework for the preparation and analysis of information for top political leadership to support their political decisions.

Taking into account analysis of systems interaction regarding others aspects of national security we could mention general challenges to establishment of a CIP system.

The problem of the credibility of information exchange system. In particular, this might present a problem when the attention of the parties involved in combating terrorism may be deliberately distracted or diverted from certain facilities (regions). This brings about ambiguity with regards to setting the level of terrorist threat between 'blue' and 'yellow' [in a specific case], which may result in underestimation of the threat and failure to provide timely preparedness of personnel and equipment involved in anti-terrorist operation (including relevant communication equipment). At the same time, the overestimation of threat and permanent high alert preparedness of the entities combatting terrorism (for example the SPPS entities) will exhaust their standby capabilities, whereas the threat information to be communicated to the public at the 'yellow' threat level will increase the relevant psychological pressure, which instead of preventing panic may lead to the outspread of panic-driven fears.

All that will objectively increase the significance of the intelligence and counter-intelligence activities and relevant agencies with regards to the terrorist threat assessment (relevant units of the SSU and MIA, Chief Department of Intelligence of the MoD, Foreign Intelligence Service, the State Border Service of Ukraine intelligence unit, and that of other entities involved in combating terrorism) and require setting up due interaction of these entities and the relevant effective (timely) information exchange, including the exchange of the state secret information.

It should be noted that the information about terrorist act threats is predominantly obtained from the intelligence and counter-intelligence sources. Also it should be taken into account that any threat information is probabilistic by nature. Therefore, when it is stated that given piece of information is credible, it shall mean that this information has been obtained from multiple sources, that, furthermore, it has been analyzed, verified and assessed to support making conclusions with regards to the probability of a potential terrorist attack (sabotage or other malevolent act).

Thus, the information about a terrorist attack can be qualified as credible only by the competent authorities, corresponding to the relevant Crisis Centers hierarchy level and different critical infrastructure sectors (energy, transport, etc) with relevant crisis response entities.

At the same time, the legislation (for example SRIP) provides very general elaboration on information exchange procedures employed, which is especially true in terms of information exchange and notifications of the leaders of the response plan participants about threats to an extent "enabling them to take decisions regarding the appropriate measures for the successful countering of such threats".

It should be stated that the availability of credible (verified) information about the threat of a terrorist act (sabotage) against critical infrastructure means that when this information is received by all the response entities in the area, these entities will still have some amount of time left to be used, first of all, for the prevention of the threat. Thus, the response process begins not when the attack on the facility occurs, (as the effective response makes it possible to prevent the attack) but fro when the important intelligence (counter-intelligence) information about the plans of attack (or about other malevolent intent) is obtained.

Another problem that may lead to the conflict of different state response systems is the issue of power and duties of the responsible body in particular type of emergency (crisis). For example, currently existing systems to be necessarily involved in the formation of response to crisis situations regarding nuclear facilities (administered by the MoECI) are inconsistent with each other both in terms of the list of entities, level of interaction coordination and centers for decision-making regarding the change of operation regimes (*Table 2.3.3*).

Table 2.3.3. **Duties of the Responsible Bodies**

System	Chief Coordinator	Operation Regime Decision Level	Party in Charge of IEI at the Facility
USSCP	SESU	The decision of executive authorities on different levels (CMU, oblast and district state administrations, local public authorities)	NPP Director General – Incident Commander or CEO of the operator
Functional Subsystem of electricity and nuclear-industrial complex	MoECI	Minister via appropriate deputy	NPP Director General – Incident Commander
Functional subsystem of the security of the nuclear energy facilities	SNRIU	SNRIU (not identified at the SNRIU level)	State Nuclear Safety Inspectorates at NPPs (through SNRIU Information and Crisis Center)
USSPRM-T	SSU (CTC)	Head of CTC with written consent of SSU Head	SSU CTC Interagency Coordination Board
SPPS	SNRIU	SNRIU (not identified at the SNRIU level)	1) Director General of NPP (licensee) – in accordance to Order of functioning on the SPPS. 2) The head of the interagency operative headquarter – representative of SSU – in accordance to SRIP. 3) Director of Operating organization – in accordance to the joint order of the MoECI and Ministry on Emergency Situation of Ukraine (currently SESU) – from 15.09.2011 № 501/1001

The **development of the new system** of prevention and response to all types of treats is problematic both due to financial and resource constrains, and from the perspective of the perception of the proposed solutions on the part of the existing state system.

In the view of this situation, it would be useful to set up an integrated system of the situation centers and coordination of existing state systems.

For the energy sector it would be useful **to establish the Energy Security Sectorial Situation and Crisis Center** in the capacity of the constantly operational separate unit in the MoECI system, which would integrate the individual systems into a coordinated system of response, interaction and information exchange, given the need to resolve inconsistencies in the existing state systems and necessity to consider threats of all types (all hazards approach) and ensure performance of the MoECI functions pertaining to:

- physical protection of nuclear facilities, nuclear materials, radioactive waste etc.; setting up of the state system of measures intended to ensure preparedness to elimination of accidents at these facilities;
- operation of the MoECI USSCP functional subsystems; response to emergency situations, radiological accidents; coordination of actions in the course of crisis situation and minimization of their consequences; development and implementation of the coordinated activities in the framework of the SRIP (took over the duties of interagency headquarters within MoECI);
- arrangements for analysis and integration of information related to the threats to critical energy infrastructure facilities, projection of probable course of events to enable appropriate response and control;
- involvement of additional personnel and equipment, as well as relevant off-site support forces (law-enforcement agencies, special forces units, the AFU units and other military units) in case of a threat at the critical nuclear infrastructure facilities exceeding the facility design basis threat;
- operational arrangements for companies, institutions and organizations of critical infrastructure (energy sector) in the special period; provisions to support operation of critical infrastructure, technical capability backup and recovery of its facilities in the special period;
- updates on the recent developments disseminated to the President of Ukraine, the CMU and the NSDCU according to the established procedure;
- arrangements for stability of critical energy infrastructure facilities operation providing functions and services, the disruption of which may lead to the most severe negative consequences for the normal life of the society, the country's social and economic development and the national security;

- arrangements for the interaction of energy systems dispatch services (electricity and gas systems) in terms of information and notification regarding the threat or actual crisis situations and disruptions in the operation of energy industry facilities, which may lead to crisis situations;
- arrangements for energy supply in the conditions of special regime period and the emergency situations in the Integrated Power System of Ukraine;

> ***Note*:** The Law of Ukraine «On Electric Energy Industry» defines an emergency situation in the Integrated Power System of Ukraine as follows: «a situation that brings about a threat of disruption of operation regime of the Integrated Power System of Ukraine or its separate parts, in particular as a result of the deficit of electric energy and/or electric power, frequency drop below the minimum admissible level, violation of the admissible power flow mode or the overload of the transmission network elements, voltage drop down to the accident level at the energy system control points».

- initiation of the special operation regimes of the Ukraine gas transportation (transit) systems taking into account the coordinated modes of joint operation of the EU countries and Ukraine;
- support preparedness of personnel and equipment involved in anti-terrorist operations and ensure necessary protection and security level of potential terrorist target facilities;
- analytical support of the President of Ukraine, the CMU and the NSDCU (through National Center for Crisis Management and Critical Infrastructure Protection and Main Situation Center of Ukraine of the National Security and Defense Council of Ukraine), as well as other entities involved in the response to crisis situations in terms of evaluation of consequences of crisis (emergency) situations and impact of that on the energy and national security.

In general, Sectorial Situation and Crisis Center (like Energy Security Situation and Crisis Center) shall become an organizational and technical venue for analytical support and coordination of actions of different response entities to crisis situations both in terms of the crisis plans activation, and in relation to the threats in the area of responsibility of other existing state systems of protection and response, as well as the issues not yet regulated by the legislation.

2.4. TRAINING AS A TOOL OF BUILDING UP RESILIENCE OF CRITICAL ENERGY INFRASTRUCTURE

The importance of resilience of a national CI was recognized few decades ago and in last few years many countries developed a range of legislation that have helped them establish reliable state critical infrastructure protection (CIP) system. The need to grant resilience of CI was emphasized by modern threats that were labeled as "hybrid warfare"[49]. Leading nations establishing CIP systems move further shifting focus on developing measures to enhance resilience of societies and countries[50].

In Ukraine, wider discussion of ways to adapt national security system to modern threats was recognized by the NSDCU decision that tasked the CMU to establish the State System on CIP.

IMPORTANCE OF THE TRAINING

Working on implementation of the NSDCU decision government agencies encountered the serious problem of interagency cooperation. The absence of working common language (terminology of different prevention, protection and response systems), unified procedures of communication

---

[49] The World Hybrid War: Ukrainian Forefront: monograph abridged and trans lated from Ukrainian / Volodymyr Horbulin. – Kharkiv: Folio, 2017. – 158 p. –Retrieved from http://www.niss.gov.ua/public/File/book_2017/GW_engl_site.pdf

[50] Commitment to enhance resilience. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw, 8–9 July 2016. – Retrieved from http://www.nato.int/cps/en/natohq/official_texts_133180.htm?selectedLocale=en

Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy. – Retrieved from https://europa.eu/globalstrategy/sites/globalstrategy/files/regions/files/eugs_review_web_0.pdf

and interactions (different systems work on their internal procedures) seriously hinders the process of establishing the CIP system in Ukraine.

The NISS, supporting work of government on the CIP Concept implementation, have organized a series of workshops and seminars discussing the problem. These discussions resulted in rising public awareness of importance of development of training programs in the area of CIP, what was later reflected in some publications[51, 52].

In expert's view Training Program on CIP have to provide potential students with knowledge of the policies, plans, methods and tools of CIP and to learn them to apply risk management techniques in analyzing and evaluating facilities as well as enhancing security and resiliency of national critical infrastructures.

One of educational training tools is collective exercise, which are the most relevant for developing common understanding of the problem by participants, who usually mostly work separately. World best practice proposed set of exercises[53]:

- **Seminar** (discussion exercise) – Seminars generally orient participants to, or provide an overview of existing strategies, plans, policies, procedures, protocols, resources, concepts, and ideas. Seminars can be valuable for gaining awareness of the capabilities of interagency or inter-jurisdictional operations and developing or making major changes to existing plans or procedures;
- **Workshop** – An exercise usually is employed to build specific products, such as a draft plan, policy, procedure;
- **Table-top** (discussion exercise) – A tabletop exercise is intended to generate discussion of various issues regarding a hypothetical, simulated emergency. TTXs can be used to enhance general awareness, validate plans and procedures, assess the types of systems needed to guide the prevention of, protection from, mitigation of, response to, and recovery from a defined incident. Generally, TTXs are aimed at facilitating

[51] Kondratov S. The problem of establishing professional development programs in the field of critical infrastructure protection of Ukraine. – Retrieved from http://www.niss.gov.ua/content/articles/files/kadry-d370c.pdf

[52] Sukhodolia O. Energy security and sustainability of energy sector of Ukraine: problems of public and corporate management // Power Engineering: economics, technique, ecology. – 2017. – № 2. – P. 124–130. – Retrieved from http://energy.kpi.ua/article/view/111710/106645

[53] Homeland Security Exercise and Evaluation Program (HSEEP) – Retrieved from https://www.fema.gov/media-library-data/20130726–1914–25045–8890/hseep_apr13_.pdf

conceptual understanding, identifying strengths and areas for improvement, and/or achieving changes in perceptions.

- **Simulation** (Games) – An exercise that often involves two or more teams, (representing a control center or management team) usually in a competitive environment, using rules, data, and procedure designed to depict an actual or assumed real-life situation. Games explore the consequences of player decisions and actions.
- **Operations-Based Exercises** (functional exercises). These type exercises are characterized by actual reaction to an exercise scenario, such as initiating communications or mobilizing personnel and resources. They are used to validate functionality of plans, policies, and procedures; personnel performance and resource sufficiency.
- **Drill** – A drill is a coordinated, supervised activity usually employed to validate a specific function or capability in a single agency or organization. Drills are commonly used to provide training on new equipment, validate procedures, or practice and maintain current skills.
- **Full-scale (Live)** – A full-scale exercise is usually conducted in a real-time, stressful environment that is intended to mirror a real incident. Personnel and resources may be mobilized and deployed to the scene, where actions are performed as if a real incident had occurred. The FSE simulates reality by presenting complex and realistic problems that require critical thinking, rapid problem solving, and effective responses by trained personnel.

The choice of exercise is stipulated by cost effective way of achieving its aim and objectives. In case of Ukraine (in times of hybrid war against Ukraine and current stage of the CIP concept implementation) seminars and table-top exercise[54] were chosen as the most appropriate form of training of involved agencies personnel and checking consistency (availability) of current plans, standards, and procedures in the field.

---

[54] Emergency planning and preparedness: exercises and training. – Retrieved from https://www.gov.uk/guidance/emergency-planning-and-preparedness-exercises-and-training

Seminar is based on an existing plan and is used to develop awareness about the plan through discussion. The emphasis is on problem identification and solution finding rather than decision making. Involved participants can be either new to the job or established personnel.

Table top exercises are based on simulation and usually involve a realistic scenario and a time line, which may be real time or may speed time up. Players who are involved interact with each other and understand the roles and responsibilities of the other agencies taking part. In TTX players are expected to know the plan and they are invited to test.

Ukrainian lessons of 2014–2016 years demonstrate the importance of critical energy infrastructure (CEI) for a national resilience. Russia utilized different tools of hybrid warfare for undermining an ability of the energy sector to provide Ukraine with energy supply. Those have included damaging of infrastructure, blocking of supply of fuel for power plants, cyber and physical attacks as well as use of propaganda to apply synergy of the effort[55].

In general, tensions between two or more countries or groups of countries can provoke attacks on energy supply system in order to destabilize society by undermining economic development and political will to withstand the deliberate aggression. Thus, an CEI comprising energy producing, transmitting and supplying elements is critical in terms of ensuring stability at political, economic and military levels and providing conditions for balanced development of a state[56].

That is why it was suggested to organize first national level table-top exercise on the issue of resilience of critical energy infrastructure. The Ministry of Energy and Coal Industry of Ukraine, working on improving a physical protection system of energy facilities, supported the training.

The idea of Table-Top Exercise on Critical Energy Infrastructure Protection (TTX) was jointly initiated by the NISS and NATO Energy Security Centre of Excellence, as one of practical steps in developing of

---

[55] Sukhodolia O. The energy dimension of war. The Ukrainian experience: An overview of the Ukrainian events in 2014–2016 // Energy Security: Operational – 2017. – № 11.

Analysis of targeted actions against CEI in Ukraine identified the following as non-military means of warfare: (1) causing psychological pressure in order to spread panic, social tension and discontent with government; (2) causing economic losses due to seizures of CEI and energy resources, thus imposing additional economic burden on the country or getting additional resources for war; (3) obtaining local advantages by achieving a better position to pursue certain operations (combat collision, terms of contracts, ceasefire negotiation) or by forcing the government to do certain actions (payments, sale or purchase of resources); and (4) creation of a desired image in international community by making information campaigns in the mass media (cruelty of Ukraine in blocking energy and water supply, «humanitarian aid of Russia» in the form of energy supplies to Ukrainian consumers).

[56] Learned lessons of Ukraine demonstrate that the damaging of critical infrastructure capability to perform its functions became one of the tools to diminish the country's ability to resist the aggressor. Malicious actions against critical infrastructure could become the tool of the state-aggressor, not just certain groups criminals (terrorist groups), as it was believed until now.

established partnership between institutions[57]. TTX was supported by Ukrainian government[58] and NATO that was reflected in Comprehensive Assistance Package for Ukraine, endorsed by the Heads of State and Government of the NATO-Ukraine Commission at Warsaw on 9 July 2016[59].

By this decision, Alliance countries provided support of Ukrainian efforts in building up national CIP system by means of sharing information and best practices in this field. The NISS and NATO Energy Security Centre developed a program of the event for wider involvement of participants not only from different Ukrainian agencies but also from NATO member countries[60].

THE CONCEPT OF TTX

The table-top exercises named as «Coherent Resilience 2017» (CORE2017) had goals:

- to check existed procedures on prevention, protection and response on incidents related to energy sector and;
- to facilitate mutually cooperation departments in theirs action to provide resilience of the National Power System, including international efforts to meet emerging security challenges.

Specific objective of the TTX was to identify the main aspects to be covered in developing contemporary Contingency plan for a Critical Energy Infrastructure – Integrated Power System of Ukraine.

The target audience of TTX was personnel of government agencies and ministries in the field of Energy, Emergency Services, National Security that included companies producing, transmitting and supplying electricity, government officials, military personnel, national police and other institutions and agencies responsible for protection and building resilience of electricity supply by improving plans, procedures and processes at a national level. The whole list of involved agencies in fact reflected list of *Table 2.3.2.* in this book.

---

[57] The National Institute for Strategic Studies and NATO Energy Security Centre of Excellence established partnership in July of 2015.

[58] The resolution of the Vice-Prime Minister for European and Euro-Atlantic integration of Ukraine dated 01.08.2016 No. 22235/3/1–16.

[59] Comprehensive Assistance Package for Ukraine. – Retrieved from http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_09/20160920_160920-compreh-ass-package-ukraine-en.pdf

[60] Advanced Training Course – "Critical Energy Infrastructure Protection". Retrived from https://www.nato.int/cps/en/natohq/news_146436.htm

The TTX was designed as multistage event that consists of: Concept and Specification Development, Planning and Product Development, Operational Conduct and Analysis and Reporting according to NATO directive[61].

At the Planning Stage there was developed a scenario with main focus on Resilience of Integrated Power System of Ukraine comprising generation, storing, transmission and distribution processes.

The scenario was designed to comprise a number of threats under all hazard approach that affect an uninterruptable energy supply. It includes natural disasters, technical malfunctions and cyber-attacks that are common in peace time as well as informational warfare, political destabilization, criminal activity that was applied to Ukraine under hybrid warfare.

The scenario planned to apply the threats to different elements of Power System affecting production, transportation/distribution and supply of energy including fuel supply for generation capacities under different stages of potential conflict of two countries.

At the Operational Stage TTX foresaw two stages: two days Academic Seminar and three days' Scenario-based discussions.

The Academic Seminar provided presentations and discussions on four topics:

- The Terrorist (Kinetic) Threats to CEI;
- The Cyber security Dimension of CEI;
- The Management System in time of Energy Sector Crisis;
- Strategic Communication in Crisis.

The discussions of every mentioned topic were structured in delivering presentation on best available in NATO countries practice and learning Ukrainian lessons in countering hybrid warfare as well as question/answers sessions on following issues:

- threats identification, risk assessment and planning for security and safety incidents and crises involved critical infrastructure;
- response, emergency and contingency plans for critical infrastructure protection;
- learning Ukrainian lessons of countering attacks against critical energy infrastructure;
- role of personnel training and education in building resilience of CEI.

[61] NATO BI-SC Collective Training and Exercise Directive (CT&ED) 075-003. Retrieved from www.act.nato.int/images/stories/structure/jft/bi-sc75-3_final.pdf

The Scenario-based discussion was divided into four phases, namely: a) pre-conflict, b) conflict of low intensity; c) high intensity conflict and d) post-conflict situation.

Participants were divided in four Syndicates and were supposed to respond on vignettes and injections within existing in Ukraine response and emergency plans and procedures with focus on different aspects: STRATCOM Syndicate (dealing with hostile propaganda and manipulations as well as crisis communication), SITE PROTECTION (dealing with cyber and terrorist attacks at CEI site level), CRISIS RESPONSE[62] (dealing with and energy crisis response on national level and interagency interaction and exchange of information), INTERCOOP (dealing with interaction and response at an international level).

Under scenario's injections participants were supposed to:

a) analyze vulnerabilities of critical energy infrastructure based on identified risks and threats,

b) determine the consequences of failure, attack and/or damage to critical energy infrastructure and impacts on other related dimensions of society,

c) determine cooperation and coordination between institutions, agencies and organizations establishing emergency services and assess their plans,

d) exercise crisis management processes, including military and civil emergency planning as a response to conditions provoked by hybrid means in pre-conflict, conflict and post-conflict situations.

The Scenario gave the option for involvement of participants from NATO countries to be directly involved into exercise by constituting separated syndicate INTERCOOP with the goal to check out available instruments of international cooperation in crisis situation in non Alliance country.

The general concept of injection introduction and syndicate's interaction under scenario-based discussions is shown on *Fig. 2.4.1*.

The Reporting Stage have had an aim to provide correct analysis of the TTX and evaluate the exercise against its stated aims and objectives as well as to identify the gaps in exciting plans and procedures (prevention of, protection from, mitigation of, response to, and recovery from a defined incident) as well as areas for improvement.

[62] In fact, this syndicate reflected tasks of proposed Energy Security Sectorial Situation and Crisis Center including responsibility of the interagency headquarters within MoECI regarding response on nuclear incidents under framework of the SRIP.

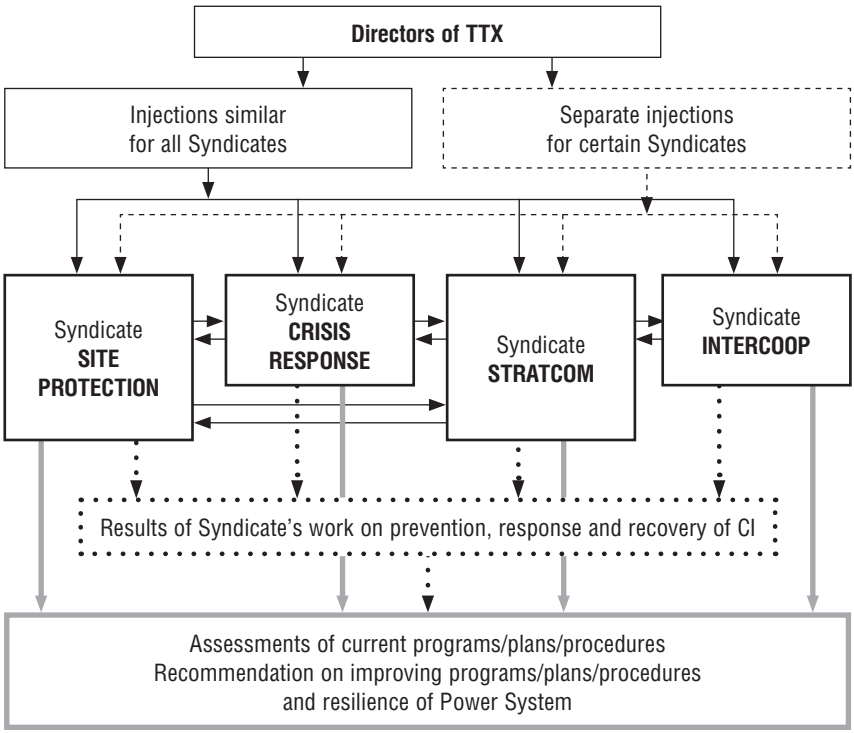


Fig. 2.4.1. **The general concept of injection introduction and syndicate's interaction**

Lessons identified, forwarded to government of Ukraine[63], increase the Ukrainian authority's awareness of the contingency planning importance as well as increase NATO's competence in supporting nations in building resilience of CEI.

PRELIMINARY CONCLUSIONS ON TTX ORGANIZATION

Conducting the TTX appeared to be effective tool to raise awareness of importance of critical infrastructure to the national resilience. More

[63] Final Report on TTX scheduled to be delivered to Ukrainian government to the end of 2017.

than hundred participants from Ukrainian government departments were involved in the process of planning and participation in TTX.

While preparing the exercise, a series of workshop was initiated and/or conducted by the NISS:

- Seminar "Establishing a system of personnel training in Ukraine in the field of CIP" (9 November 2016), conducted by the NISS together with PDP NATO in Ukraine;
- Workshop "The main approaches to planning of actions in the event of a crisis situation on objects of critical energy infrastructure" (13 April 2017), conducted by the NISS;
- Workshop "Best practice of public relations in the event of serious incidents on critical infrastructure objects" (11 May 2017), conducted by the NISS;
- Workshop "Critical National Infrastructure (19–23 June 2017), conducted by the UK Cabinet Office Emergency Planning College;
- Workshop "Critical National Infrastructure: Energy Sector (4–7 September 2017), conducted by the UK Cabinet Office Emergency Planning College.

The exercise in fact became an effective tool to build inter-agency networking and to establishing common understanding of the main problems that have to be resolved. TTX have helped the understanding that an effective cooperation between the government and the private sector is needed for enhancing resilience of national critical infrastructure.

At the same time the TTX have demonstrated that Ukraine needs an effective governance – nationally, at industry and individual organization level, to set goals and monitor progress towards them.

The Government has to take the leading role in establishing the State CIP system including through approving earlier mentioned Concept for building a state CIP system in Ukraine (see chapter 1.3) and appointing responsible body for its implementation. Particular tasks of a CIP system differ from the tasks of the existing state systems (civil defense, counter-terrorism, cyber threat counteraction etc.) and that is why establishment of a National Center for Crisis Management and Critical Infrastructure Protection (NCCM&CIP) as a separate body to be responsible for coordination and exchange of information.

PART III

FURTHER STEPS IN DEVELOPMENT OF CRITICAL INFRASTRUCTURE PROTECTION CONCEPT

3.1. THE ROLE OF PLANNIG IN CIP SYSTEM FUNCTIONING: SOME IMPLICATIONS FOR UKRAINE FROM THE REVIEW OF BEST PRACTICES IN THIS FIELD

According to widely recognized modern approaches to protection of critical infrastructure (CI), it includes various objects, systems, networks (both physical and virtual) chosen for their vital importance for nation livelihood that their damage or incapacity would lead to quick and severe consequences for safety and security of public, national economy and national security or any combinations of these matters.

The scale of the impacts which could emerge as a result of CI operation failures due to any reasons and resources which could be allocated for CI protection and resilience are the key criteria when assigning one *object or system, or network* (hereinafter referred to as "object") to CI. Taking into account this consideration it becomes clear that only a smaller part of all infrastructure objects will be assigned to the category of (national) CI, namely – only those security and safety incidents at which could potentially lead to a crisis situation of the national level because in case of undue response its impact can easily expand far from one or another CI sector causing so called domino and cascade effects.

The scale and complex character of consequences caused by crisis situations at the CI objects, necessity to provide protection and to ensure a due level of CI resilience raise urgently the issues of coordination, interaction and exchange information (IEI) among numerous stakeholders of CI protection including responding to security and safety incidents at the objects[64].

[64] Hereinafter in the specific context of the topic the term «responding» will be used in a broader meaning covering all complex of measures beginning with preparation measures and ending with mitigation of consequences and restoration of operation of CI objects.

One cannot resolve these issues if stakeholders have not agreed plans and established procedures for cooperation, IEI. The same could be said if the plans and procedures no more than paper exercises, in other words, if plans and procedures robustness and efficiency for any reasons are not subject to testing either under real conditions or during training (exercise) efforts of different levels, and, therefore, even formal grounds are absent to improve such plans and procedures. Basing on the above considerations the following security maxim may be formulated: "No robust plans to respond to security crisis, no system to respond exists".

The following sections of the paper present briefly the best foreign practice in this field taking, mainly, the U.S. National Planning System (NPS) as an example; the overview of the situation with planning process in Ukraine in terms of national approaches compliance with those applied in the developed countries, and some specific proposals for improvement Ukraine's planning capabilities to adequately respond to incidents and crisis associated with CI objects[65].

When writing the paper the findings of discussions occurred 13 April, 2017 at the NISS during the joint meeting of the *Interagency expert working group on counteraction WMD proliferation, terrorism and critical infrastructure protection* and the *Working group on cooperation with NATO in the field of energy security* on the topic "*The main approaches to plan actions in the case of a crisis situation at the critical energy infrastructure objects*".

ON MODERN APPROACHES TO PLANNING FOR CRISIS SITUATIONS BASING ON EXAMPLES FROM BEST FOREIGN PRACTICES

As a rule, planning is an integral part of the system management process including such a system as national security which, in its turn, covers activities aiming at CI protection and resilience. In the most developed countries relevant programs and plans are subject to approval

[65] The event was carried out within the framework of preparation for the first in the history of independent Ukraine the TTX of the national level aiming at testing interaction of national/state crisis response systems in the case of incidents and crisis associated with the critical energy infrastructure (for more detailed information see Chapter 2.4. and seminar at the NISS about the event (in Ukrainian): http://www.niss.gov.ua/articles/2549/)

by legislative and normative acts of the national level. Really, for example in Poland the *National Critical Infrastructure Protection Programme* (2013) and its updated version (2015)[66] were approved by the Polish Government in pursuance of Article 3 (2) of the Law "*On Crisis Management*" (2007).

Another example – in Czech Republic the issue of planning for crisis situations was resolved by adoption in 2010 of the amendments of the law № 240/2000 "*On Crisis Management*"[67]. The above mentioned amendments regulate activities in the field of CI protection and provide for, inter alia, development of relevant plans by central authorities, the National Bank, the law enforcement bodies and the special services, as well as local governments of Czech Republic.

Although the experience of the Central and Eastern European countries neighboring Ukraine is very valuable for Ukraine, further the main attention will be paid to the U.S. experience because this country is an undisputed leader in developing and introduction of modern approaches to ensuring national security, in general, and CI protection and resilience, in particular, as well as in the field of crisis responding[68]. The U.S. NATO allies and a number of European countries not being Alliance members when establishing relevant national systems rely mainly upon the approaches developed and best practices used by the United States. The study of American experience in this field allows of identifying the parameters of the "corridor" within which national practices will likely develop in the nearest future.

Some important for Ukraine implications from U.S. National Planning System Overview with regard to CI protection and resilience

In the U.S. activities in the area of CI protection and resilience are carrying out within implementation of National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and

[66] National Critical Infrastructure Protection Programme. – Retrieved from http://rcb.gov.pl/en/critical-infrastructure/

[67] On Crisis Management. – Retrieved from http://www.hzr.cz/hasicien/article/crisis-management-in-the-czech-republic.aspx?q=Y2hudW09Mg%3d%3d

[68] For the purpose of this publication the term «crisis response systems» means all national/state systems designed for responding of all stakeholders to security and safety incidents and crisis.

Resilience[69] (its previous versions dated 2006 and 2009), which was developed in pursuance of Presidential Policy Directive – 21 (PPD-21)[70].

At the moment, there is a sophisticated well-developed planning system in the U.S. which is relying on a number of interrelated conceptual and legislative documents providing a systematic approach to planning at all management levels, all jurisdictions and for all stakeholders of the planning process. More detailed information is accessible on the site of the U.S. Federal Emergency Management Agency (FEMA)[71] which has become a part of the U.S. Department of Homeland Security since March 1, 2003 as one of the results of the institutional measures undertaken by the U.S. Government following the September 11, 2001, attacks.

In terms of planning issue within the framework of activities toward CI protection system creation in Ukraine one could highlight the following important features of the NPS:

1. The framework of the NPS is created with a set of interrelated consistent conceptual, legislative and regulatory documents providing a systemic approach to planning at all management levels, for all jurisdictions and all categories of stakeholders involved in responding to incidents and crisis situations caused by threats and hazards of any origin.

2. The NPS provides application of common terminology and a unified approach to planning for all threats and hazards that is consistent with the widely recognized principles for a planning process and envisages active involvement in cooperation and participation in joint planning of all stakeholders across the society.

3. When planning, all threats and hazards and their any combinations are taken into account; the planning process includes all interrelated mission areas – *Prevention, Protection, Mitigation, Response and Recovery*[72].

4. "The NPS includes two key elements: the *Planning Architecture*, which describes the *strategic, operational,* and *tactical levels* of planning and *planning integration*"[73] (*vertical* and *horizontal*, as well as the

[69] NIPP 2013: Partnering for Critical Infrastructure Security and Resilience. – Retrieved from https://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf

[70] Presidential Policy Directive – Critical Infrastructure Security and Resilience. – Retrieved from https://fas.org/irp/offdocs/ppd/ppd-1.pdf

[71] U.S. FEMA, National Planning System – Retrieved from https://www.fema.gov/media-library/assets/documents/114298

[72] See note 71.

[73] See note 71.

Planning Process. The levels of planning usually fall into two categories – *Deliberate planning* and *Incident action planning,* as well as the *Planning Process* including 6 main steps of planning based on widely recognized general approach to planning activities.

5. The NPS is characterized by deep and wide integration of planning efforts including vertical and horizontal integration of planning activities across the whole community.

6. Planning of incident and crisis management is, in fact, one of the tools for risk management. The best practice for this purpose envisages involving as much public servants, law enforcement and intelligence officers, experts, specialists in different disciplines, etc. as possible. When doing so, well-defined priorities, goals and objectives allow ensuring unity of a purpose, coherence and consistency of actions of all stakeholders even when responding to large-scale complex crises.

7. The planning in this field is an on-going process, i. e. plans are implemented and maintained, refined and improved continuously for a number of reasons including but not limited to findings received from exercises or actual incidents/crises; within a framework of routine scheduled maintenance; changes in risk posture or in law, policy, etc.; organizations use training events, exercises, and real-world incidents to assess the effectiveness of plans and to improve them.

8. The major requirements for the planning process (periodicity, terms and conditions for reviewing, responsibilities for plans development, implementation and maintenance are regulated by legislative and normative acts of different levels.

Bearing in mind these U.S. best practice peculiarities the situation in Ukraine is briefly analyzed below. However, it is important to remember that attempts to mechanically copy foreign experience not taking into account national specificity, as a rule, lead to setbacks.

THE CURRENT SITUATION IN UKRAINE REGARDING CRISIS PLANNING IN TERMS OF CI PROTECTION AND RESILIENCE

First of all it should be noted that Ukraine is still at the very beginning of establishment of a modern comprehensive responding system to address security and safety incidents and crises involved CI. At this point, in terms of CI concept introduction our country is, at least, 15–20 years

behind the U.S. and 10–12 years behind such its neighbors, as Czech Republic and Poland.

Really, the term "critical infrastructure", was defined in the Ukrainian legislation only in 2016. And it is symptomatic that it was made by the Ukrainian Cabinet of Ministers' decree which addresses *critical information infrastructure*, being the part of the CI although a very important one[74]. The matter is that delay in establishment of CI protection system became an obstacle for development of other sectors and subsectors of the national security, and one of them – security of critical information infrastructure.

What is more, the relevant decision of the NSDCU, enacted by the Presidential Decree addressing CI protection issue was not fully implemented within the period of time prescribed by the document[75].

At the moment, the state/national protection systems as well as crisis response systems available in Ukraine are focused on their "own" threats and risks, and, therefore, to a large extent autonomous while plans and procedures (if any) to ensure interaction among systems are either insufficiently developed or almost declarative in nature. Virtually, there are several national systems[76] in operation and one – under its establishment relating to CI protection.

To illustrate insufficient or declaratory interaction of the listed above systems their operation modes are compared below for the hypothetic case when ***confirmed information is available concerning the threat of a terrorist act against a CI object*** which could be resulted in serious negative consequences for lives and health of public not only due to use of fire-arms and explosives by terrorists but also due to damages of process equipment installed on the site, i. e. in case of realization of different threats combination (a complex threat).

---

[74] Decree of Cabinet of Ministers of Ukraine of 23 August 2016 № 563 «On approval of the Procedure for creation the list of the information and communications systems of the State's critical infrastructure». – Retrieved from http://zakon.rada.gov.ua/laws/show/563-2016-п

[75] See the Decision of the NSDCU «On improvement of measures to ensure pro tection of critical infrastructure objects» enacted by the Presidential Decree of 16 January 2017 № 8/2017 which envisaged development and approval of the Concept for es tablishment of the Critical Infrastructure protection system and development and ap proval of the Law of Ukraine «On Critical Infrastructure and Its Protection» by the mid of 2017.

[76] These systems mentioned before: USSCP; USSPRM-T; SPPS; NCCS.

Table 3.1.1. **The operation modes/conditions/levels of three Ukrainian systems in the case of threats combination realization**

USSCP **Operation modes**	**SPPS** **Operation conditions**	**USSPRM-T** **Levels of terrorist threats**
daily operation	*normal operation*	
		grey (possible threat) *in the case of factors (conditions) facilitating terrorist acts commitment are in place*
high readiness	*high readiness*	
		blue (potential threat) *in the case of available information on planning to commit the act of terrorism requiring a confirmation*
		yellow (probable threat) *in the case of reliable (confirmed) information on preparation for terrorist act commitment is available*
emergency situation	*operation in a crisis situation*	*red* (real threat) *in the case of terrorist act commitment*
state of emergency		
	restoring the normal operation	

When considering the *Table 3.1.1* presented attention should be paid to the following:

1. Relevant regulations on the systems under consideration use different terms to describe operation modes, namely «modes», «conditions» and «levels».

2. In fact, one can say that almost complete coincidence is observed only for the first two operation modes of the USSCP and the SPPS which, actually, can be treated as the most simple in terms of planning and responding[77].

3. Unlike other two systems, the USSPRM-T has no a mode which could be put in correspondence with the modes of *daily* or *normal operation.*

4. The more complicated modes the more is incompliance of the criteria of their introduction. Thus, for the case chosen as an example

[77] The lack of consistency of the terms including their scopes is the main reason that majority of the modes included in the table has no exact matches with those of other two systems.

(*the threat of a terrorist act with possible serious consequences for lives and environment)* the systems would operate in the following modes:

- USSCP – daily operation mode[78];
- SPPS – operation in a crisis situation[79];
- USSPRM-T – the mode adequate to the penultimate, *yellow level* on the terrorist threats scale[80];

It can be confidently assumed that in a real situation the USSCP will be after all involved in responding to a complex threat including terrorist, man-made and ecological components. But this example is quite persuasive to demonstrate that the Ukrainian legislation in force cannot be a firm basis for authorities and other organization when planning joint response actions, interaction and cooperation among relevant state/national systems. Really, development of effective plans of interaction and coordination for such a case requires, at least, terminology harmonization, determination of correlations among different modes of systems operation, agreeing management principles for different stages of a crisis (including clear line responsibilities distribution among all stakeholders, procedures to transfer overall management of responding operations, etc.) since a complex crisis is associated with the impacts of a number of dangerous factors.

Summarizing the above considerations, one could state that in Ukraine the issues of providing CI protection and resilience, in general, and planning relevant interaction and coordination, in particular, to a large extent are due to the fact that ***no one of the systems listed above is designed to respond to all types of threats*** that resulted in the lack a systematic approach to CI protection at the national level taking into account extensive interdependencies of CI elements and considering CI as a single, although overcomplicated, object of protection.

One of the implications of this situation is that there is no Ukrainian authority/body responsible for CI protection and resilience as a whole, i. e. on the supra-ministerial level. In the author's opinion, it was one of the reasons of the failed attempts to introduce in Ukraine the widely

[78] According to the regulation on the USSCP the system will respond only during a state of emergency when numerous terrorist acts have been committed caused fatalities and destruction of vital infrastructure objects.

[79] In fact, that is the state of system's highest mobilization since the next category of conditions is assigned to the *conditions of restoring normal operation*.

[80] As for the *color scale* of terrorist threats introduced in Ukraine, it is unclear, why the highest (*red)* level of the terrorist threat is established and the threat of a terrorist act is treated as *real* one only after terrorist act commitment?

recognized so called the *all hazards approach,* since those attempts were executed by the authorities charged with operation of one of the crisis response system focusing only on a certain range of threats.

This statement can be underpinned by the example of creation of the State Extraordinary Commission[81]. As stated in Paragraph 1 of the regulation on this Commission, this Commission "is a permanent body providing coordination of activities of the central and local authorities associated with ensuring technogenic and ecological safety, public protection against emergency situation consequences, ***organizational measures to counteract terrorist activities and military threats***, prevention of emergency situations and responding to them". Thus, all types of threats are mentioned in paragraph 1 of the regulation, but hereinafter in the text one could not find any more reference to the term "terrorism" and derivatives from it, none of the further paragraphs mentions procedures of interactions with the USSPRM-T. At the same time, other parts of the document are narrated in a spirit of responding to natural and man-made hazards that is typical for the State Emergency Service of Ukraine which was charged with drafting the document.

It is understandable that counterterrorist measures require very careful attitude to publication of documents relating to relevant activities, and one could suppose that there are some sensitive interagency regulations addressing issues of coordination, interaction and information exchange. But even if they are, in the light of best foreign practices, it is necessary for Ukraine to consider the possibility of publication of "open" versions of such documents. Otherwise, in the absence of relevant publicly available information it will be very difficult to achieve common understanding of goals and objectives, use of agreed terminology, integration of efforts of all stakeholders, including authorities, private companies and people, to protect CI and to ensure a due level of its resilience. It is in that context that the crucial role might be played by a set of conceptual and strategic documents forming a firm basis for planning activities across the society.

SOME CONCLUSIONS AND RECOMMENDATIONS

Basing on the best practices and analysis of some examples describing the situation with the planning in the field of CI protection and ensuring

[81] Decree of the Cabinet of Ministers of Ukraine of 26 January 2015 № 18 «On State Commission on Technogenic and Ecological Safety and Emergency Situations». – Retrieved from http://zakon2.rada.gov.ua/laws/show/18-2015-%D0 %BF/paran13#n13

due level of its resilience in Ukraine the following conclusions are drawn and recommendations put forward:

1. Bearing in mind the leading position of the U.S. in this field and nation's influence on approaches and methods applied in other developed countries including NATO allies as well as some European nations, it is reasonable for Ukraine to make the most of U.S. experience in introduction of a systematic approach to the planning process and the relevant procedures when building up a critical infrastructure protection system in our country.

2. The analysis of the planning issues in terms of CI protection and resilience, interaction of the national/state crisis responding systems currently available in Ukraine reveals that the Ukrainian legislation in force is not in position to ensure due level of interaction among the systems because of absence of a profile legislation including lack of agreed goals and objectives, as well as coherent terminology, because of each system's focusing on a specific range of threats (i. e. dismissing the *all hazards approach*) and absence of a central authority charging with coordination of activities aiming at protection and ensuring a due level of CI as a whole.

3. Planning is an integral part of the process of CI protection and ensuring resilience, and relevant efforts should be integrated both vertically and horizontally across all society providing for as wide involvement of public servants, law enforcement officers, specialists of different discipline, etc., etc. as possible.

4. Relevant legislative and normative acts to be approved in Ukraine shall include specific provisions on the planning activities specifying responsibilities distribution, periodicity of plans reviewing and testing including during exercises and trainings, other terms and conditions defining planning activities at all levels of management.

5. The Ukrainian authorities should consider the possibility to introduce the practice of development and publication of the "open" versions of strategic and conceptual documents addressing issues of CI protection and resilience.

6. After the first breakthrough step in this field, namely the Decision of the NSDCU "On improvement of measures to ensure protection of critical infrastructure objects" enacted by the Presidential Decree of Jan 16, 2017 № 8/2017 Ukraine urgently need to fully implement all measures provided for this document, and, first of all, development and approval of the Law of Ukraine "On Critical Infrastructure and Its Protection", basic for this domain.

3.2. ON SOME CONSIDERATIONS FOR INFORMATION EXCHANGE AND BUILDING THE DECISION MAKING SUPPORT ARCHITECTURE TO PROTECT CRITICAL INFRASTRUCTURE IN UKRAINE

Because of CI specificities its due protection and resilience require involvement of numerous actors across a State and society, representing different authorities and agencies, state and private companies, local communities, NGOs, experts, media, population, etc. In this connection, it is understandable that in activities aiming at strengthening CIP and resilience special attention should be paid to coordination, interaction and information exchange (IEI) among all parties involved, from the leadership of a State to its ordinary citizens, from the government to local authorities, and so on.

Bearing in mind that Ukraine is still at the very beginning of establishment of its CIP system, creation of a relevant IEI system is also on the agenda. The latter one will also serve as a tool for supporting the decision making processes at all levels of management including the highest political one. Despite Ukraine is yet preparing to develop the profile legislation on CIP some general provisions to the IEI system are already defined in the conceptual documents.

Really, NSDCU's decision «On the concept to develop the national security and defense sector of Ukraine» enacted by the Presidential Decree № 92/2016 of 14 March 2016 provides for creation of both the Main Situation Center of Ukraine and the (National) Situation Centers Network as the tools designed to improve «information and analytical support and to minimize time needed for making important management decisions»[82].

[82] Decree of President of Ukraine «On implementation of the decision of the National Security and Defense of Ukraine № 92/2016 of 14 March 2016 «On the Concept to develop the national security and defense sector of Ukraine». – Retrieved from http://zakon3.rada.gov.ua/laws/show/92/2016

Here we put forward some recommendations on how to establish the IEI system and to improve information and analytical support in the field of CIP. Basing on the major goals and objectives of a CIP system and the provisions of the above mentioned presidential decree while bearing in mind the best practices and widely recognized approaches to information processing cycles some important considerations regarding IEI system and information and analytical support to the decision making process in Ukraine in this field are presented below.

THE OVERVIEW OF THE CURRENT SITUATION REGARDING IEI IN TERMS OF CRITICAL INFRASTRUCTURE PROTECTION IN UKRAINE

The current situation in Ukraine regarding IEI in terms of CIP can be characterized as that wherein departmental approaches are dominated. It means that the available national/state systems for emergency responding, crisis management and objects protection are almost exclusively relied upon agencies' missions and responsibilities to ensure proper responding *to the certain types of threats and risks* paying insufficient attention (if any) to those lying beyond their direct mandates. The principal consequences of such a departmental approach are the following: (1) even if, according to the statute, a relevant system has the status of national/state, its functionality, virtually, has been limited by the level of a ministry/agency responsible for system operation; (2) deriving from the previous, there are no robust procedures for informing and involving the highest political level and the major actors of other systems designed to respond to other types of threats and risks; (3) despite some IEI procedures are formally foreseen in plans, actually they have never been subject to testing during trainings and exercises at the levels higher than object (facility) ones; (4) within the framework of such approaches there is no place to public-private partnership, one of the pillars, of the national critical protection systems in developed countries[83].

[83] NIPP 2013: Partnering for Critical Infrastructure Security and Resilience. – Retrieved from https://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf

To underpin the above statements let us consider three existing national/state systems in operation which shall respond to security incidents and crises at the nuclear facilities to be certainly assigned to CI namely: USSCP; PPS; USSPRMT.

The conclusion on insufficient or declaratory IEI among the listed above systems can be easily derived from comparing their operation modes at different security and safety conditions, as it is made in chapter 3.1[84].

Hypothetic case of «confirmed information concerning the threat of a terrorist act against a nuclear facility» quite clearly shows that the national legislation in force cannot be a firm basis for IEI procedures and mechanisms, especially at the higher management levels.

It can be concluded that the problems associated with CIP and resilience in Ukraine to a considerable degree can be attributed to the fact that none of the currently available national/state systems is designed for responding to *all threats and hazards*. Another result stemmed from the current situation is that no Ukrainian authority/agency deals with CI as a whole, that is, at the supra-ministerial/agency level, while it is a body that should be at the top of the pyramid describing the IEI processes and procedures to ensure the proper level of CIP and resilience against all threats and hazards.

But, before development, introduction and verification of the IEI procedures, protocols, mechanisms, etc. it is necessary to reach the agreement on the common terminology, to determine correspondences among modes, conditions, and levels defining system operation regimes, to establish crisis management principles and distribution of responsibilities at different stages of a responding process (including procedures for the responsibility transfer) since roles of the actors may change when responding to an incident/crisis, etc.

The approaches to the IEI processes and procedures and some consideration regarding the architecture of the relevant system are discussed in the next section.

---

[84] As it is argued in the hypothetical case of availability of confirmed information concerning the threat of a terrorist act against a nuclear facility which may be resulted in serious negative consequences for lives and health of public not only due to use of fire-arms and explosives by terrorists but also due to damages of process equipment installed on the site, i. e. in case of realization of a different threats combination (terrorist, man-made, and ecological ones).

INTELLIGENCE INFORMATION CYCLE AND INFORMATION AND ANALYTICAL SUPPORT TO A DECISION MAKING PROCESS

Considering the possible ways to establish a CIP system and relevant sub-systems, as IEI one, proper attention should be given for using as much as possible the available capabilities and resources. In the specific context of the subject matter it means that existing systems designed to respond to certain threats and risks should be integrated and incorporated into a single system aimed at CIP. Such a goal can be achieved, inter alia, through considerable improvement of procedures and mechanisms for ensuring coordination, interaction, and information exchange among the systems available to be implemented basing on a new legislation addressing CIP and resilience.

At the same time, the above mentioned improvements are possible only within a framework of a new system designed to protect critical infrastructure including IEI sub-system relying upon the National Situation and Crisis Center Network (NS&CCN) with the Main Situation Center of Ukraine (MSCU) at its top position. Bearing in mind quite a numerous number of different situation, information and analytical, crisis centers functioning under different authorities, businesses, jurisdictions, institutions in our country, at this point it is necessary to identify approaches to these centers integration and incorporation into the NS&CCN basing on their functions and capabilities.

A possible option to identify such an approach could be provided by the *FBI intelligence cycle*[85] (or similar ones) adapted to the Ukrainian conditions regarding CIP.

The intelligence cycle process model can be of use for the Ukrainian case because (1) it represents the information process model applied by such an authoritative agency as the FBI; (2) description of the stages (elements) of the cycle allows structuring IEI processes and procedures within the Ukrainian NS&CCN.

At this point it is necessary to underscore that when reforming the national security sector in Ukraine much more attention should be paid to arranging information and analytical support to the decision making

[85] Stokes, Roger L. Employing the intelligence cycle process model within the Homeland Security Enterprise. Monterey, California: Naval Postgraduate School. – Retrieved from https://calhoun.nps.edu/bitstream/handle/10945/39018/13Dec_Stokes_Roger.pdf?sequence=1

process especially to its analytic and prognostic components. Sometimes, it is the analytical stage that is missed in the information process cycle when raw data and information are directly sending to higher levels of management, including the highest political level, thereby ignoring the fact that the time available for the State leadership is a very limited resource.

Thus, when building up the system designed to support a decision making process regarding security and resilience of the critical infrastructure and the NS&CCN the following steps (elements) of the information processing cycle should be taken into account:

1. Requirements.
2. Planning and direction.
3. Collection.
4. Processing and exploitation.
5. Analysis and production.
6. Dissemination.

Relevant powers, functions, and responsibilities with regard to IEI procedures should be distributed among all available systems and their actors while integrating them into a single CIP system designed to adequately respond to all threats and risks. When so doing, the NS&CCN is believed to be a main tool in providing the decision making process with information and analytical support.

Bearing in mind the recent cyber-attacks against the CEI objects in Ukraine[86] and the growing cyber threats posed by our country's enemies when creating the NS&CCN continued focus shall be made on the due level of cyber- and information security within the network.

THE INFORMATION EXCHANGE PYRAMID AND SUPPORT TO DECISION MAKING PROCESS

It shall be noted that Ukraine established national and sectoral systems to combat certain types of threats, including crisis management in case of their implementation. As part of operation of these systems there are specified IEI mechanisms, including through situational-crisis center (SCC) specially created for this purpose – see *Table 3.2.1*.

[86] E-ISAC report «Analysis of the Cyber Attack on the Ukrainian Power Grid», March 18, 2016. – Retrieved from https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

Table 3.2.1. **Levels and Subjects of IEI within NS&CCN in nuclear sphere**

Hierarchy of IEI	Structural elements/subjects of NS&CCN	The role and functions in IEI (According to informational cycle stages)
Political level	President of Ukraine, NSDCU, CMU	*Stages 1–2 of an informational cycle:* requesting about certain information, strategic planning and management of resources according to threats and tasks. *Stage 6 of an informational cycle:* obtaining needed information for decision making process; forming the next request
1st level of NS&CCN	SCC on national level: MSCU and SCCP within NSDCU	*Stage 6 of an informational cycle:* the final analysis, training, developing and submitting the required form of alternative strategic and political decisions regarding the crisis; exchange information with other national SCC (if established) – horizontal level of IEI; exchange information with 2nd level of NN SCC – vertical IEI
2nd level of NS&CCN	SCC at ministerial (branch) level (according to main groups of treats and fields of response): State Center for Emergency Management (SEMC) within USSCP; Center of prediction consequences of radiation accidents at the State Hydrometeorological Service; CTC SSU; Ministerial Situation and Crisis Center (at the MoECI); ICC SNRIU; Emergency Disaster Medicine Service Center of Ukraine within MoH; State Center for Cyberdefense and Prevention of Cyber Threats (SCCP); SCC in MoD and MIA	*Stage 5 of an informational cycle:* analysis, evaluation and verification of data and information; unification and merger of information for mutually agreed (as possible) a picture of the crisis development; preparation of recommendations for a set of options in decision-making to respond crisis and mitigate the effects of the crisis; exchange information with 1st and 3rd level of NN SCC – vertical IEI. exchange information on 2nd level of NN SCC – horizontal IEI; briefings for media, analysts and experts, communities, NGO

Hierarchy of IEI	Structural elements/subjects of NS&CCN	The role and functions in IEI (According to informational cycle stages)
3rd level of NS&CCN	SCC and ICC of national level monopolies: NAEC «Energoatom»; NEC «UkrEnergo»; «UkrHydroEnergy»; «Ukrtransgas», «Ukrtransoil», Etc. Dispatcher (informational) services of Law enforcement units (MIA) and AFU, MoD as well as units of Emergency Services (SESU) at local level	*Stage 4 of an informational cycle:* processing and formatting of the primary information in order to present it in a form suitable for use by analysts, including preliminary synthesis of information; adding an information to specialized databases; exchange information with 2nd and 4th level of NN SCC – vertical IEI; exchange information on 3rd level of NN SCC – horizontal IEI
4th level of NS&CCN	SCC and ICC of enterprises and facilities of critical infrastructure (licentiates): internal and external CS of NPP; Control centers of technological process safety (for nuclear industry – the control and monitoring of nuclear and radiation hazardous objects, especially reactor systems); Dispatcher (informational) services of Law enforcement units (MIA) and AFU, MoD as well as units of Emergency Services (SESU) at object level	*Stages 2,3 of an informational cycle:* collecting primary information and subsequent transfer of information by various ways and means of including: from control and monitoring systems; from staff and personnel; from primary units of respond at the facilities; from individuals among the population (through national systems, emergency communications and emergency); from law enforcement, emergency services and others from the place; exchange information with ICC SNRIU and other ICC of enterprises and facilities of critical infrastructure – horizontal IEI; exchange information on 3rd level of NN SCC – vertical IEI
Public level	Population, MM, expert groups	On the one hand at this level could form and primary signals and primary information (raw) about the threat or beginning of the crisis around the nuclear facility or other CI facility, on the other hand, public safety is one of the highest priorities for crisis response. Media and expert community should facilitate this process, which shall include, without limitation, the following: providing information for 3rd and 4th level of NN SCC – vertical IEI; exchange information with media and experts, communities– horizontal IEI

For example in nuclear sphere, the SRIP provides for activation of the situational/crisis centers of the agencies involved to ensure needed IEI procedures. *The lowest level of such a network includes NPP's site monitoring and control systems* for the various security parameters of facilities (including industrial, nuclear, radiation and physical) as well as monitoring systems controlling the environment, weather conditions and so on. Each NPP has an internal information-crisis centre (ICC), external and backup external ICCs, which are intended for administration of the emergency forces at the NPP site and are usually located in the NPP sanitary protection zone as well as in the surveillance zone. This level of the network is very important in terms of obtaining raw data, which subsequently will be the subject to processing and analysis to support the decision-making process. At this level, direct exchange of information between partners in responding activities is carried out and serves as a basis, mainly, for a tactical decision-making process.

The next hierarchical level of the IEI system – *operating organization level* – shall include SCC and ICC of large companies having the CI objects. In particular, this level covers mostly implementation of tasks assigned to *Step 4* of the cycle of information preparation – that is, processing, formatting and, partially, initial analyzing information and data to transfer to partner structures (horizontal exchange) and to a higher hierarchical level. It is this level that during a crisis operational and tactical decisions are making at. From this level information is transmitted to operational personnel and first responders to support their actions.

Next hierarchical level of IEI system – ministerial/departmental level – shall include SCC and information & analytical centers of ministries/departments:

- the State Emergency Management Center (SCEM) of SESU (its creation and operation is provided for by the Code of Civil Protection) – emergency situations of natural and technological disasters, civil protection, elimination of consequences of emergencies, including those at nuclear facilities;
- the CTC SSU (its establishment and functioning is provided for by the Law of Ukraine «*On Combating Terrorism*») refers to countering terrorism, including its nuclear and radiological types;
- the crisis units at the MoECI (the necessity in their operation is provided for by both regulations on the USSCP and relevant functional subsystems of the MoECI, and by the SRIP (i. e., within USSCP and

USSPRM-T) regarding technical nuclear safety, ensuring nuclear security, international cooperation in the nuclear field[87];

- the Information Crisis Centre of the SNRIU deals with nuclear safety and security issues including regulation in the nuclear field, international cooperation (including informing the IAEA about nuclear safety and nuclear security incidents;
- the Ukrainian Scientific and Practical Centre of Emergency Medical Care and Disaster Medicine deals with organization of emergency medical aid in crisis situations;
- the State Centre for Cyber Protection and Combating Cyber Threats (SCCP SSSCIP) deals with combating cyber threats.

Establishment of crisis response structures at the MoD and the MIA (the National Guard and the National Police) is also provided for in the Ukrainian legislation since these authorities play due roles in the first response to emergency situations of different origin, provision of nuclear security, physical security of other CI objects.

Also, it should be noted that in accordance with the Ukrainian legislation in the event of crisis, inter-ministerial/inter-departmental structures (centers, committees, etc.) are created to ensure IEI at different levels of management. These structures are usually headed by the local authorities of the appropriate level or CMU's top officials. Such structures should be included in the CIIE procedures and their participation in crisis response actions should be taken into account in the SCN architecture as well.

At the national level the principal situational emergency response centre of the state, providing direct information and analytical support of decision-making at the highest political level, is the Main Situation Centre of Ukraine (MSCU) under the NSDCU. National Coordination Center for Cyber Security of the National Security and Defense Council (NCCCS) of NSDCU also corresponds to this level.

In conclusion, in our view, the establishment of the National Situation and Crisis Center Network (NS&CCN) will provide reliable and timely information of political top management of the state in crisis situations and improve CI security.

---

[87] Authors arguing the necessity of establishment of Energy Security Sectorial Situation and Crisis Center of the MoECI that have to be tasked with wider range of duties. See Chapter 2.3.

***Note*:** Before transferring to the political level, information needs to be processed, formatted, validated, analyzed, etc. Nevertheless, the state leaders should have diversified technical capabilities for information directly from the place of crisis.
Based on the existing normative acts and national experience with crisis response to Level 2 include interagency committees that usually creates in case of crises of various kinds. The activity of such organized structures, usually supported by the agency, which is specialized for a particular type of crisis.

It should be noted that the crisis structure of the MoECI, as is prescribed by the legislation within the USSCP and other functional systems of the USSCP as well as within the SPPS and the USSPRM-T, to date, are not properly established. For example in energy sector, their duties partly are put at dispatcher centers of MoECI and some Energy companies (operators of energy facilities). Therefore, in authors' view it is reasonable to establish the Energy Security Sectorial Situation and Crisis Center (SSCC) of the MoECI to monitor on an ongoing basis (24 hours a day, 7 days a week,) potential crisis situations in the energy sector and to interact with the network of national, sector and corporate situation and crisis centers (situation, crisis, crisis information, information and analytical and control centers operating in the crisis or emergency) that will become an integral part of the Center's activities.

The SSCC of the MoECI have to be determined by:

- a threat level: available information regarding threats of any nature, including information of the different degree of credibility;
- a phase of crisis situation evolution: initial response, operation during crisis (emergency) or recovery period (elimination of consequences);
- a legal regime in the country: state of emergency, special regime state.

According to suggested CIP concept there have to be established 4 stage operational regime of a CIP system:[88] normal operation mode; high alert (responding to emerging threats), crisis situation and consequences mitigation (recovery of operation), as well as operation in the

[88] See Chapter 1.3.

conditions of the state of emergency (special regime) introduced in the whole country or in the separate regional areas.

The SSCC functions and tasks pertaining to the threat response, prevention of threat realization and elimination of consequences will change respectively as described below:

Normal Operation Regime: to collect, systematize and analyze data related to the CI facilities, assessment of risks from threats of all types both for the individual regions as well as for the county as the whole; to monitor potential crisis (emergency) situations related to the operation of CI; to provide expert assistance to the government agencies, CI operators; to ensure information exchange; to form proposals related to improvements of the regulatory framework of CIP.

High Alert Operation Regime: to provide continuation of all normal operation regime activities; apart from that additional arrangements shall be made: implementation of the supplementary preventive, security and organization measures at the CI facilities (enhance security and access-control, protection of data and information, form reserve and back-up capabilities for emergency response, etc); to put response personnel and equipment on the stand-by; verify preparedness of the response personnel and equipment; to forecast probable consequences of the threat realization based on which the SSCC shall develop recommendations for other participants; to develop possible measures to stabilize situation; to permanently monitor evolution of the threat-related events.

Crisis Operation: to ensure implementation of the supplementary activities, in particular: situation assessment (scale of potential consequences, need for additional personnel and equipment); to coordinate activities intended for minimization and elimination of crisis situation consequences; to implement operation stabilization measures regarding CI sectors; to activate back-up capabilities; to provide information to the CMU, NSDCU and the President of Ukraine on recent developments. In this regime some SSCC could be defined as a technical venue for the activities of the State Extraordinary Commission

Recovery Regime: to provide coordination of activities intended to restore functionality of damaged CI, assessments of needs and coordination of efforts of state agencies and CI operators and public involved in recovery activity; to brief government, international institutions and public on recent developments.

Obviously, the elements (centers) of the SCN will exchange certain information on a regular basis under any security and safety conditions

but if needed a specific request (requirement) for certain information will trigger the intelligence process cycle addressing a specific threat or hazard. Other options may be associated with acquisition of intelligence information on terrorists' plans, alerts caused by different man-made and natural disasters and so on. Let us briefly consider the information cycle steps and actors' roles proposed in a specific case when a relevant input comes from the highest political level.

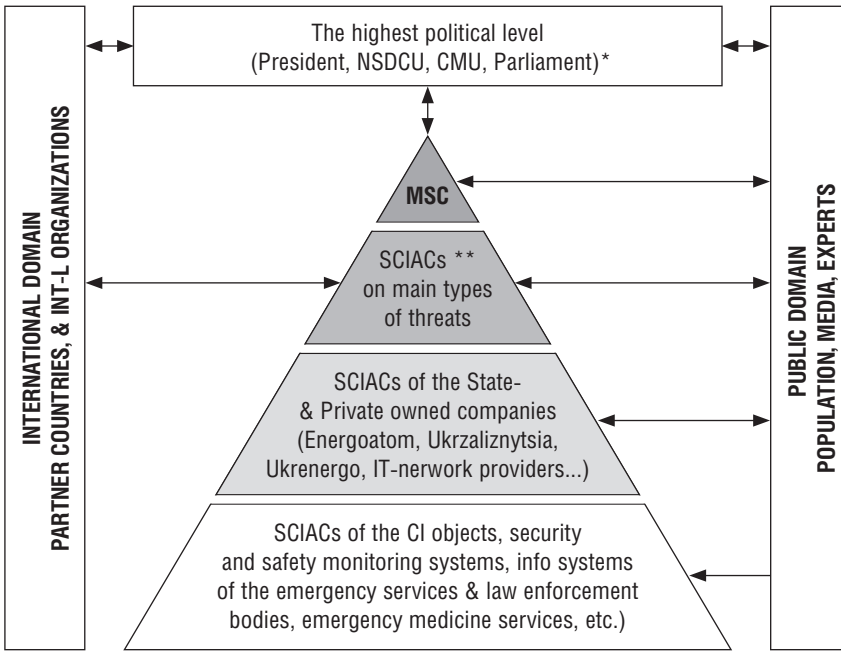
Basing on the above mentioned strategic documents of a national level, it would be logical to assume that it is the Main Situation Center of Ukraine (MSCU) established at the NSDCU that occupies the top of the information exchange «pyramid» created on a basis of the National Situation and Crisis Center Network (NS&CCN).

On the other hand, at the time of writing, the security sector of Ukraine is under conditions of deep reforming so it is necessary to take into account other options for the MSCU belonging to other actors at the highest political level (e. g., President, CMU). In case of establishment of several centers at the political level attention should be paid for clear responsibilities distribution among them (e.g. for critical infrastructure security and cyber security being heavily overlapped areas). In any case, the MSCU should be established to reliably involve the political leadership of Ukraine in IEI procedures on national security and defense issues including those relating to CIP and resilience.

When adapting the FBI intelligence cycle model to the Ukrainian conditions one could imagine the following sequence of the steps and relevant actions.

So, in the case under consideration the intelligence information cycle is launched by the input from the highest political level (see *Fig. 3.2.2*). Basing on the input ***requirements (requests) for certain information (Step 1)*** are formulated by MSCU. MSCU should be an institution where such requirements (requests) are formalized, formatted and distributed among the parties involved being responsible for other steps of the process. Thus, the MSCU will execute ***Step 2 (the planning and direction***) to determine the type of information and resources needed, the way and timetable to collect it. Besides, deriving from the input the MSCU will determine the format of a final product to be submitted to the customer at the end of the cycle.

Step 3 (information collection) should be the main responsibility of the situation, crisis, information and analytical centers of the CI objects and systems, and the function of security and safety indicators



** The listing order reflects the actors' roles in ensuring national security*
*** Situation, Crisis Information & Analytic Centers*

Fig. 3.2.2. **The information exchange pyramid**

monitoring systems, information systems of the emergency services and law enforcement bodies, emergency medicine services and so on. As for intelligence information, the main sources of it include but are not limited to information sources from intelligence and law enforcement communities, news reports, open-source documents, etc. Besides, raw information may be directly received from the public domain. In case of security and safety incidents information collected should be used to support tactical operations of first responding teams.

Step 4 (processing and exploitation) includes converting the raw data into formats usable for analytical efforts, data translation and decryption, interpretation of filmed images and other imageries, converting data stored on different media into usable for analysts information, entering data in specialized databases and so forth. It is reasonable to

charge with this objectives the situation, crisis, information and analytical centers of the major state and private companies, operators of the CI, such as Energoatom, Ukrzaliznytsia, Ukrenergo, Ukrhydroenergo, etc. Moreover, the relevant centers at this level could be charged with preliminary analysis of information received. In case of response such information should be used to support the decision making process at the operational level.

Step 5 (analysis and production) covers information verification, integration, and analysis to create as concerted the picture regarding a problem (situation) as possible to include it in the final product. Such efforts require highly professional personnel passed relevant training. In author's view, it is reasonable for analysts to identify a range of recommendations on possible options for further steps concerning the issue triggering the information request or, for example, scenarios to resolve a crisis. This level of the pyramid should include the major situation centers dealing with the main types of threats and hazards. As of the situation in Ukraine, the centers belonging to or operating by, at least, the following ministries/agencies should be assigned to this category:

- the SESU (according to legislation in force, deals with emergencies caused by man-made and natural disasters);
- the SSU and CTC SSU (terrorist threats);
- the MoD (military threats, terrorist threats);
- the National Guard of the MIA (physical protection of nuclear facilities and other objects to be assigned to critical infrastructure);
- the MIA (fight against crime and threats to public order);
- the SNRIU (ensuring nuclear safety and security, monitoring conditions at the nuclear facilities, other radioactively dangerous objects);
- the SSSCIP (cyber threats and information protection);
- the Ministry for Public Health of Ukraine (threats to public health, emergency health-care services, disaster medicine, threats to biosecurity, etc.).

Of course, this list is not exhaustive and may require clarifications, especially in the course of security sector reforming. Besides, because in Ukraine the practice to establish interim inter-ministerial/interagency bodies in case of emergency situation (crisis) is provided for by the national legislation care will be taken to integrate information units of such bodies into the NS&CCN. When so doing, the later should be assigned to this particular level of the information exchange pyramid. Information

and data produced therein can be also used for strategic planning and management regarding CIP and resilience.

Step 6 (final evaluation and dissemination) will include final analysis and evaluation of information regarding the request/situation, developing and submitting in the required format alternatives of political leadership's decisions on actions to resolve issues. This stage may include repeated requests/demands either of new or additional information for clarification follow-ups triggering a new information process cycle. Obviously, at this step cyber- and information security measures shall be the most rigorous.

The role of the public domain in information exchange in crisis situations has been traditionally underestimated in Ukraine so far. At the same time, it is impossible to achieve a due level of CIP and resilience without involvement of all actors across the society. It is especially true with regard to responding measures, mitigation of crisis consequences, and recovering CI objects operation and functions. One more aspect to be taken into account is that the public domain may be a valuable source of raw information about threats, risks, emergency conditions, etc. At the same time, in authors' view, it is reasonable to exclude information transmission to the public domain without relevant verification and processing since raw information may be mistreated and cause disruption and even panic among the population.

Information exchange with partner states and international organizations is to be carried out to meet the commitments of Ukraine according to international agreements and treaties. As a rule, the competent authorities responsible for relevant information exchange belong to those operating national/state systems focusing on certain threats. Thus, information produced during ***Step 5*** can be used for these purposes. In all other cases, a special decision at the political level shall be made to disseminate information to foreign governments and relevant international organizations.

In order the NS&CCN plays a due role in supporting a decision making process all its levels should be vertically and horizontally integrated to provide a unified approach to CI&IE procedures and mechanisms across the society activities aiming at CIP and resilience.

Basing on the analysis made and bearing in mind the best practices of support to decision making process it is necessary to make the following **conclusions**:

1. The existing Ukrainian systems designed for crisis and emergency responding, and protection cannot provide a due level of protection and resiliency of the objects to be assigned to the national CI. The same is true for the current information and analytical support procedures and mechanisms to underpin decision making processes at all management levels including the highest political one.

2. Among the main reasons of the above mentioned situation are:

a) domination of the departmental/ministerial approaches to crisis management characterizing by governmental bodies' focus on their «own» threats and hazards and reluctance to deal with those beyond their direct responsibilities; and related;

b) ignorance of the *all hazards approach* widely recognized and recommended for application in this field in the developed countries;

c) insufficient PPP in the security sector, in general, and in the field of CIP, in particular;

d) within the frameworks of existing in Ukraine procedures and mechanisms to support decision making processes, especially at the highest political level, insufficient attention has been paid to stages at which information should be analyzed, evaluated, summarized, properly formatted, etc.

Taking into account the recent conceptual documents and legislative acts approved in Ukraine and basing on the above findings some recommendations regarding information and analytical support to decision making processes in the field of CIP should be made. They are the following:

1. A systematic approach to establish procedures and mechanisms for information and analytical support to decision making processes with regard to CIP should be applied involving the NS&CCN and the MSCU operation of which is envisaged by the Presidential decrees.

2. At this historic period NS&CCN and MSCU creation and further operation should be based on the resources and capabilities available which result in necessity to integrate numerous situation, crisis, information and analytical centers at the different levels of management, for all types of ownership, and under different jurisdictions in a single system – the NS&CCN with the MSCU at its top.

3. The architecture of the NS&CCN should reflect the relevant stages of information processing (e. g., like in the FBI intelligence cycle).

4. The NS&CCN should be well integrated horizontally and vertically while its performance should be subject to regulars testing, exercising and improving.

3.3. METHODOLOGICAL ASPECTS OF CRITICAL INFRASTRUCTURE IDENTIFICATION AND PROTECTION

Awareness of the global trend towards the intensification of negative processes initiated by both man and nature, increase of terrorist threats, number and sophistication of cyber attacks, dramatic events in the east and south of Ukraine in 2014–2017 have mainstreamed the problem of protecting the country's infrastructure, which is vital for the safety of public, society and the state. This infrastructure is internationally identified as critical.

The countries, which use the term «critical infrastructure» (CI) under the framework of ensuring their national security, understand this infrastructure as the one including the facilities, resources, and systems being so important for ensuring vital functions of their people and state, that their unstable operation, not to mention their collapse, would cause serious negative or even catastrophic consequences. Therewith, of a particular danger are cascading effects, when a malfunction of a CI facility would result in operational failures of other systems and facilities due to their interdependence (a domino effect). On the other hand, CI also includes severely hazardous production facilities, and accidents at these sites caused by any reason (natural or man-caused emergencies, wrongdoings) can also produce catastrophic consequences.

It is noteworthy that the world leading countries consider the necessity to secure their CI against all types of threats (*the all hazards approach*). At the same time, understanding the impossibility to ensure an equally high level of security for an entire CI against all possible threats has brought the development of a security approach that is focused on a selective protection of certain CI items against a limited set of known and relatively predictable threats, and the priority is given to one or

another infrastructure element depending on its «criticality» degree. And the principal measure of criticality is ***the risk***.

There exist different approaches to the definition of risk. The generalized approach to CI risk assessment includes the following:

- Identification and classification of threats and probability (or, more precisely, frequency) assessment for each threat;
- Vulnerability assessment for each type of events/attacks (consideration of a threat frequency defines hazard probability);
- Impact assessment (for various scenarios of events development).

The experience in natural and man-made emergency response, analysis of their consequences allows risk ranking of CI basing on threats. On the other hand, use of the experience gained by leading industries in assessing terrorist threats is also relevant. In particular, this applies to the experience in such areas as nuclear safety and security, aviation security, cyber security. However, not the entire infrastructure, which is critical for society and the state, is of interest to terrorists, as a target that can ensure achievement of their goals.

TERRORISM AS A THREAT TO CRITICAL INFRASTRUCTURE

Although terrorist and other malicious attacks pose a serious threat on CI, they are not as widespread as technological accidents or natural disasters. For example, according to *the Global Terrorism Database*, a relatively small number of attacks (up to 10–15 %) were targeted at CI, while most of the attacks were directed against people. Such a choice of terrorists can be explained by the fact that most of the CI sites, attacks on which could provide really catastrophic consequences, are not at all unprotected targets, while crowds of people in public places are vulnerable to terrorist attacks.

However, terrorist threats to CI can hardly be considered overblown due to the following factors:

- Along with a direct impact on CI, terrorist attacks usually cause secondary consequences, i. e. a cascade of operational disorders at other CI components;
- Terrorist attacks are pre-planned attempts to achieve a maximum impact on society and are intentionally designed to destabilize it; the secondary effect of destabilization is more important for terrorists than a direct impact on CI;

- Terrorists can try to gain control over major infrastructural facilities, which will further cause greater destabilization;
- A growing diversity of vulnerable CI objects significantly complicates identification of most probable targets for terrorist attacks and performance of relevant counter-terrorism measures;
- Security upgrades at certain CI facilities (for example, at NPPs) simultaneously increase probability of terrorists switching to other, less protected and more vulnerable sites (for example, thermal power plants that at low temperatures could provide a no less significant destabilizing effect).

In order to ecognize attractiveness of CI facilities for terrorist attacks, it is necessary to understand motivation of terrorists during their choice of a target. These motives can vary greatly, and the most typical are as follows:

- Attempt to cause mass death of people;
- Cause economic (ecological, socio-political, etc.) damage;
- Cause anxiety and insecurity;
- Get larger socio-political concern.

Generally, it comes down to the intentions of terrorists towards obtaining socio-political destabilization and an opportunity to influence a situation in a certain country or group of countries. It is the destabilizing effect that is the main goal and measure of success for a terrorist attack.

Under the conditions of hybrid warfare against Ukraine, actions of subversive groups can be stated to be among the greatest threats to its CI. That is why assessment of terrorist threat is an important element of the CI protection system development. If to take into account the cascading effects, when operational disturbances at a CI facility cause failures at other systems and facilities due to their interdependence thus resulting in destabilization in the country, then the attractiveness of large power facilities to terrorist attacks becomes clear. Hence, serious consideration should to be given to the increased intensity of cyber attacks being implemented within the CI of Ukraine. Therefore, ensuring anti-terrorism and cyber security of CI is among the key tasks of the state, and this task is in the demand of a unified system approach at the national, administrative and facility levels.

Establishment of a state counter-terrorism system in Ukraine constituted a response to terrorist threats. The conceptual and legislative framework of national counter-terrorism policy was formed at the state level. To this end, the CMU has approved the provisions on USSPRM-T system pursuant to the Law of Ukraine «On Combating Terrorism».

The Security Service of Ukraine (SSU) has been designated to be the main body within the national counter-terrorism system. The Antiterrorist Center at the SSU is a coordinating body of this system.

THE PROBLEMS OF TERRORISM THREAT ASSESSMENT

It is worth noting that the above-mentioned classical approach to risk assessment cannot always be put into practice with regard to terrorist threats. For instance, it is possible to estimate probability (frequency) for some categories of terrorist attacks basing on database indicators (for example, *the Global Terrorism Database* or *RAND Database of Worldwide Terrorism Incidents,* and *the Repository of Industrial Security Incidents* (*RISI*) for cyber attacks); and only assumptions about their frequency can be made for others. That is, the process of terrorist risk assessment is characterized by significant uncertainty, which is mostly affected by evaluation of a threat. Actually, previously developed models and estimates for natural and man-made emergencies can be used to assess consequences of terrorist acts. However, it is impossible for the assessment of terror threats, because information on the goals, motives and possibilities of terrorists is required. And while possibilities and tactics of terrorist actions can be predicted to a certain extent, estimation of a CI facility that could be a target can only be very approximate.

On the other hand, application of statistical data is also hindered by the fact that terrorist threats are derived from availability (vulnerability) and value of a particular facility (full effect), as well as from its adequate assessment by terrorists.

In addition, attention of the counter-terrorism efforts can be intentionally deflected and switched from one facility (region) to another. This implies uncertainty in assessing a level of terrorist threat. On the one hand, this may lead to an underestimation of a threat and untimely readiness of the forces and resources involved into an anti-terrorist operation. On the other hand, overestimation of a threat and permanent higher preparedness state of terrorism fighters exhaust their forces; and psychological pressure on public is being increased by the information about a threat that has to be brought to people. Then, instead of panic prevention, this can result in a contrariwise spread of panic.

The above-mentioned factors objectively mainstream role of intelligence and counter-intelligence bodies and operations in a terrorist threat

assessment and require establishment of a clear IEI between them, including the data that constitute a state secret.

THREATS TO THE CI AND FORMATION OF SECURITY PASSPORTS FOR CI FACILITIES

It should be borne in mind that hazards to CI are not limited to the terrorist threats. The *all hazards approach* requires consideration of the threats of man-made and natural origin.

For instance, the current «technogenic pressure», i. e. density of enterprises, pipelines and communications, in Ukraine is several times higher than that in most European countries. Under these conditions state regulated, standardization on security issues during emergencies and critical situations, expert review of facility projects on technological and physical security, supervision and monitoring, certification of the facilities security are essential.

In particular, the Law of Ukraine *«On Extremely Dangerous Objects»* requires security declaration for a highly dangerous facility (the document presenting analysis results for a hazard level and risk assessment of the facility; establishing a series of measures taken by a business operator in order to prevent accidents and ensure preparedness for containment and elimination of accidents and their consequences). «Provisions on Passportization of Potentially Dangerous Facilities» envisage identification of such facilities and their passportization, i. e. preparation and issuance of the passport of a potentially dangerous facility (PDF). PDF passport is a document presenting general data on a facility, data on dangerous natural conditions and technological processes, data on main hazards and emergency recipients (i. e. the objects and people, which would be affected by accident consequences), emergency response and rescue documentation, etc. Formats of PDF passports correspond to certain types of economic activity of the facilities (coal mine, hydraulic facility, major pipeline, hydrocarbon deposit, etc.).

Similar measures are envisaged in the Russian Federation; in particular, as for security of the facilities within the fuel and energy complex[89]. At the same time, security passport of an energy facility in

[89] Federal Law of the Russian Federation of 21.07.2011 № 256-FZ «On Security of Fuel and Energy Complex Facilities». – Retrieved from https://ohranatruda.ru/ot_biblio/ot/146990/

Russia presents not only its characteristics in terms of potential hazard of a facility (hazard levels derived from the properties of hazardous substances used in the facility, impact of adverse factors that may occur in case of an accident at the site), but also possible consequences resulting from unauthorized interference with the facility operation, evaluation of the condition of technical and physical protection systems, measures to ensure anti-terrorist security. Also, the data contained in a security passport are classified as restricted information.

As far as anti-terrorist security of nuclear and power facilities in Ukraine is concerned, a series of documents is being prepared basing on the vulnerability assessment results and within the framework of the SPPS. Essence of the documents corresponds to PDF passport, but these documents are much broader and more systematic in terms of hazard assessment. For instance, in addition to the general data on a facility and identified sources of danger, the Vulnerability Assessment Report contains description of threats, scenarios of offender behavior and analyzes ability of physical protection system and a facility's interaction plan to counter the threats.

We may generally state that in terms of its organization, the state system of physical protection (covering nuclear facilities, nuclear materials, radioactive waste, other sources of ionizing radiation) that is currently existing in Ukraine is among the most advanced state systems of response and security. It involves the whole chain of actions to ensure security; starting with hazard assessment, identification of a design basis threat, categorization of system objects and towards establishment of specific requirements to physical security systems, assessment of site vulnerability, risks of consequences, inspections of physical protection systems and interaction plans. Similar approaches may be used in the development of a state system of CI security in Ukraine; particularly, in the development of a «DBT», being the basis for the identification of against whom and against what it is necessary to protect CI facilities, the threats (hazards) against which the state system of critical infrastructure security should be developed.

It should be noted that identification of the DBT for nuclear facilities and nuclear materials in Ukraine is based on the IAEA recommendations on physical nuclear safety and on the analysis of modern security environment that takes account of significant changes in the security situation. Therewith, a DBT within the PP system is based on

the «offender model», which is further the basis of the «threat model» development. These models form source data for the development of security policies and design of any security systems.

Therefore, in terms of the facilities physical protection, the threat model is based on the offender model, which is being developed with the objective to get answers to the following *questions*:

- Against whom to protect?
- What is a potential offender's purpose (Reasons and motives, goals at the site)?
- Who can be a potential offender (one person or a group of people)? Is he an external or internal offender, or possibly they are acting in cahoots?
- What knowledge and skills does an offender have (regarding both the facility inclusive of its physical protection system, and the use of weapons, communications and intelligence tools, for example, drones, transport, etc.)?
- What methods and means are used by an offender (armament, technical equipment, communications, intelligence, transport vehicles, etc.)?
- What tactics can be used by an offender during his actions (action scenarios)?

At the same time, threats to CI should be also considered with regard to identification of the elements, at which the threats are directed at the protected site:

- *Physical elements*; particularly, site process equipment and resources;
- *Control systems*; particularly, automatic control and technological processes administration systems, communication systems, security systems (including access control, engineering and technical security equipment, etc.);
- *Personnel*; particularly, dispatchers, operational personnel directly ensuring a CI facility operation, security personnel, etc.

However, such threat models and the resulting DBT, which is based on the offender model only, does not provide an opportunity to develop a system of critical infrastructure protection against the threats of all types, i. e. of any origin and orientation.

Consequently, as far as the protection of critical infrastructure is concerned, the model of threats to CI is a broader concept and is based on the search for the answer to the question «What factors can cause damage to the operation of a CI facility?».

And this implies the necessity to analyze not only potential offenders, but also a CI facility: where the facility is located (including geographical, climatic conditions, its seismicity), what potentially hazardous technologies are used on the site, where and how its equipment is located, how the equipment can be accessed, what can affect its operation, what other facilities are located next to the site and can be subject to impact-generating effects, what is the facility's role in production chains, who is the consumer of its products (i. e. interdependence with other facilities), etc.

At the same time, a model of threats to a CI facility will not be complete without a detailed modeling of the socio-political situation under which it is operating, because the possibility to implement certain war and socio-political threats depends on it.

Hence, an adequate model of threats to a CI facility should include the offender model, facility model, and model of situation. In view of the foregoing, the model of threats can be presented in the following form, refer to *Fig. 3.3.1*.

Pursuant to the all hazards approach, this model takes account of the threats (hazards) of any origin: natural and man-made (are considered during a facility model development), socio-political and military (are considered during developing a model of situation), wrongful acts – cyber threats, sabotage and terrorist threats (are considered in the offender models).

Therewith, it should be borne in mind that these models (of situation, facility, offender) are interrelated and interdependent. For example, the model of a facility is the basis for identifying potential goals of an offender (including the ones related to cyber-attacks); and the socio-political situation in a state, its region or at a facility affects motives (protest moods, etc.) and actions of offenders (for example, roadblocks, etc.).

DEFINING PARAMETERS (CRITERIA) FOR THE CRITICALITY ASSESSMENT OF INFRASTRUCTURE ELEMENTS

Unlike the facilities of nuclear infrastructure, which categorization is actually guided by one criterion, i. e. hazard posed by nuclear or radioactive materials; definition of the criteria by which other facilities should be classified as CI is a much more complicated task. NISS experts proposed the following hierarchical model of the criticality definition criteria, see *Table 3.3.1*.

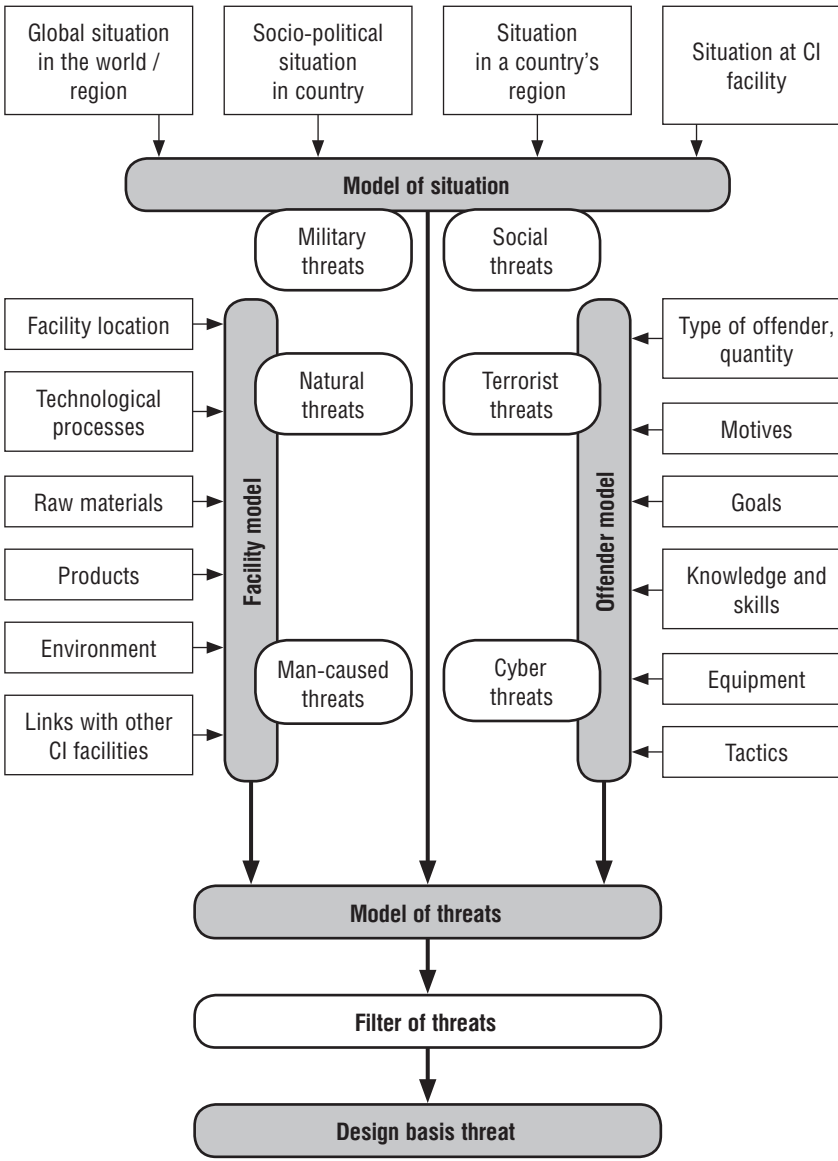


Fig. 3.3.1. **The model of threats and design basis threat for CI facilities**

Table 3.3.1. **Hierarchical model of the criteria to define criticality of an infrastructure**

Level 1	Level 2	Level 3
interdependency between the elements of critical infrastructure	cascade effects	reduced scope of functions of dependent systems
		onset of severe negative environmental, economic, socio-political consequences
		impossibility to eliminate consequences of a critical situation (operations of emergency and rescue services, provision of emergency assistance to public, etc.)
	flexibility (diversification)	possibility to deliver services/ resources from other sources (in other ways)
	redundancy	availability of redundant productions/ resources
magnitude of impact	territorial extent	local, district, regional, entire state territory, global
	magnitude of incident in organizational aspect	at the level of a process, enterprise, sector of economy, state or group of states
impact in time	time lapse before negative consequences arise	immediately, after several hours, weeks, months
	duration of effect	up to several hours, days, weeks, months, years
	time for recovery	several hours, days, weeks, months, years
severity of possible consequences	damage to health and life of people	number of affected, injured, dead, evacuated individuals
	level of disturbance of people's normal living conditions	power supply
		water supply
		sewerage and garbage disposal
		supply of basic products (food, hygiene products, etc.)
		health care services
		transport connection

Level 1	Level 2	Level 3
severity of possible consequences	economic damage	impact on GDP
		amount of economic losses, both direct and indirect ones
		number of personnel and people dealing with the facility operations
		share of the facility's product in its national production/consumption
	level of disturbance of continuous provision of the functions ensuring operational activity of strategic enterprises	stop of continuous productions
		share of the facility's product in its national production/consumption
	level of impact on financial and banking system	share of the facility in national scope of banking or financial services
	environmental damage	impact on public (contamination of air, water, food, etc.)
		impact on the natural environment
	socio-political damage	causing damage to the authority of state
		level of panic, protest and anti-state sentiments
		public anxiety, loss of confidence in authorities capacity, dissension
		symbolic value of sites (historical and cultural values)
	level of impact on state security and defense capability	disturbed governability of a state or region
		mass violations of law and order
		reduced combat readiness and combat capability of armed forces
		impact on combat capabilities (value of products/services)
		disclosure of state secrets, confidential science-technical and commercial information

It should be noted that correct quantification of the most abovementioned parameters is extremely difficult, or even impossible.

Application of expert assessment methods (estimation of current level of parameters by attributing parameter values to certain subgroup), subjectivity of decisions, uncertainty of clear critical values of indicators and heterogeneity of their evaluation scales require **application of fuzzy logic apparatus**.

AN EXAMPLE OF USING FUZZY LOGIC TECHNIQUES TO DEFINE A CRITICALITY LEVEL OF INFRASTRUCTURAL FACILITY/FUNCTION

1) **Determination of criticality assessment parameters**

A set of criticality assessment parameters for infrastructural facilities/functions was formed based on the parameters of the criteria hierarchical model in *Table 3.3.1*. Experts used a set of 16 parameters of level 2 to analyze infrastructural facilities.

2) **Determination of parameter relevance**

Relevance (significance) of the parameters that ranges from 0 to 100 % (from 0 to 1.0) was determined for each parameter using the Delphi method of expert assessment; and the sum of all parameters relevance was 100 % (1.0).

3) **Determination of parameter values**

The Delphi method of expert assessment was used to determine fuzzy value of the parameters for an infrastructural facility subject to evaluation. The linguistic change of 5 terms (*see Fig.3.3.2*) was used: neglectable (1), insignificant (2), relevant (5), significant (4), and critical (3).

4) **Visualization of results**

To visualize criticality of a facility subject to evaluation, a petal diagram was developed with its petal width corresponding to the relevance (significance) of a parameter; and the parameter's fuzzy value for a facility was defined by the experts through using the aforementioned linguistic change of 5 terms. The value of aggregated (integral) indicator of criticality (corresponds to the petal diagram area) was calculated, and its normalization was carried out (presented within the range of 0–1.0). The result of criticality assessment for a facility subject to evaluation is presented in *Fig. 3.3.2*. The facility with an integral criticality index of 0.604 was classified as «extremely important».

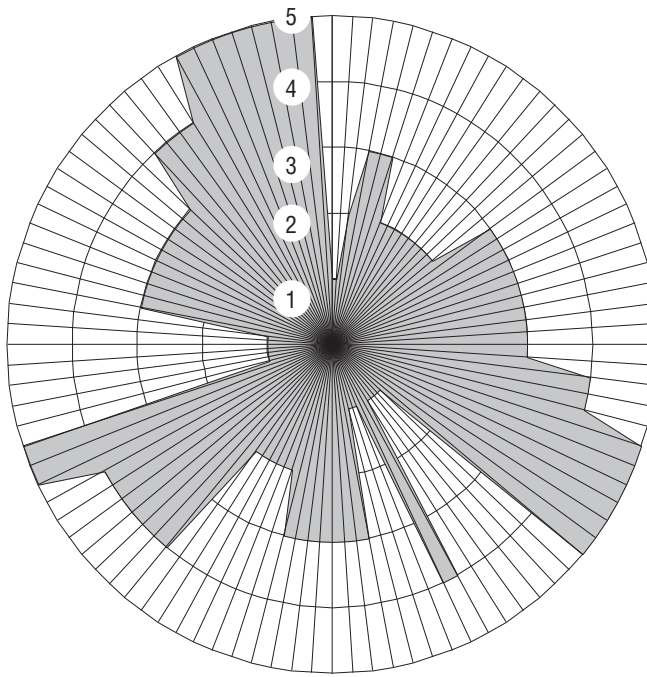


Fig. 3.3.2. **Criticality assessment for a conditional facility of CI**

5) **Ranking of CI facilities**

All infrastructural facilities shall be ranked according to calculated values of the normalized aggregate (integral) indicator. An example of ranking is shown in *Fig. 3.3.3*. To carry out linguistic recognition of an infrastructural facility's criticality level basing on the terms «vital», «extremely important», «important», the following scale was used:

Category I. Vital CI facilities: the normalized criticality factor exceeds 0.8. Large infrastructural facilities of national importance that have extensive links and significant impact on other infrastructure; measures for their recovery require extensive resources and time. These facilities should be provided with a physical protection system adequate to the threats (for example, NPPs, oil refineries, large hydrogeneration complexes, etc.). State and operators (owners) should bear responsibility for the protection of this CI in a consolidated manner; intercourse and interaction should be clearly regulated.

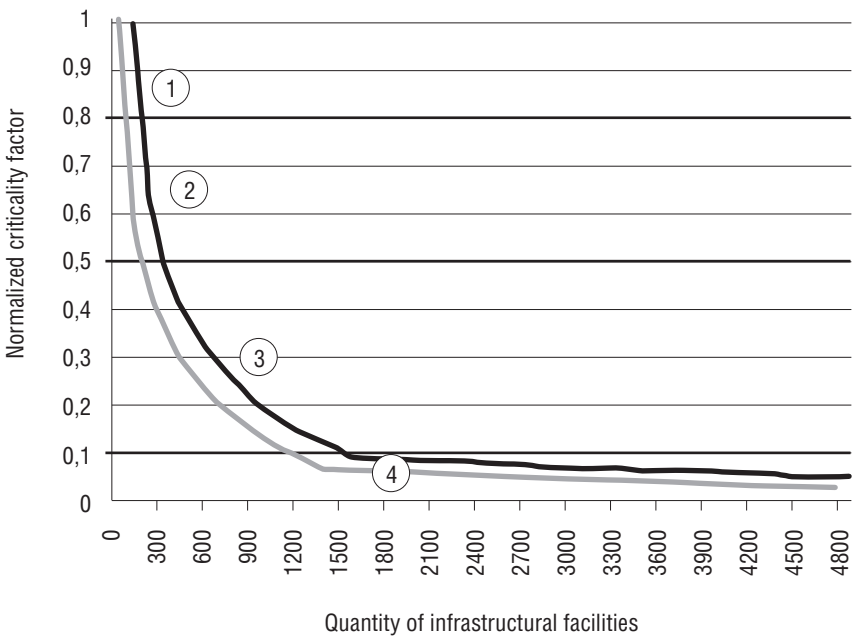


Fig. 3.3.3. **Example of infrastructural facilities ranking based on their «criticality» level**

Category II. Extremely important CI facilities: the normalized criticality factor ranges between 0.5 and 0.8. These facilities should to be provided with both physical protection measures and ability to quickly restore their functions through diversification and redundancy (for example, large petroleum tank farms, underground gas storage facilities, electric power substations, bridge transitions, large elevators, drinking water sources, etc.). Responsibility for the protection of this CI should be borne by operators (owners) and state and should be based on public and private partnership; strict state control over compliance with safety regulations and requirements should be ensured.

Category III. Important CI facilities: the normalized criticality factor ranges between 0.1 and 0.5. The main way of this infrastructure protection is prompt recovery of its functions through diversification and redundancy (for example, thermal power plants, highways, etc.). First and foremost, operators (owners) should bear responsibility for the

protection of this CI, and state should ensure availability of the conditions for its diversification and redundancy.

Category IV. The facilities, which normalized value of aggregate (integral) indicator is below 0.1, were not referred to critical infrastructure; immediate protection of these facilities is the sole responsibility of their operator (owner).

It should be noted that the reference criticality values (0.1, 0.5 and 0.8) assumed in this example were provisionally estimated by the experts and should be refined based on the assessment results for the major part of infrastructural facilities, also including a state's capacity.

CONCLUSIONS AND RECOMMENDATIONS

To date, protection of critical infrastructure in Ukraine was actually understood as ensuring security (physical protection), which is dealt with under certain services and departmental units, or as protection against man-made and natural emergencies, which is dealt with under the SESU. The more global issues, which are related to ensuring resistance of CI facilities to any threats and the ability to ensure performance of their functions for life-support of people, society, businesses and the state in the event of these threats implementation at the state level, are not dealt with under any department at the systemic level.

Green Paper recommendations indicate the necessity to develop a law of Ukraine on the protection of critical infrastructure, which among others would identify the subjects and structure of a CIP system. Therewith, in order to ensure the system's further development, we need an administration unit to coordinate the development of legal, organizational, methodological, technological and other CI protection tools, ensure rapid analysis of existing threats and risks, and develop recommendations to the government on operation modes of a CIP system depending on the level of threats and legal status.

3.4. PROSPECTS FOR ESTABLISHING THE ENERGY RESERVE

The Green Paper covered a wide spectrum of issues related to CIP. This Paper combines analysis of the situation in Ukraine regarding solving tasks of protecting individual groups of CI facilities and analysis of experience of critical infrastructure protection system development in the world's leading countries.

Events of 2014–2015 increased urgency of protection of infrastructure, objects and systems vital for the activity of the society and created a need to establish a CIP system for Ukraine. Uncertainty of the current historical moment opens a corridor of additional opportunities for our country to reduce the lag from the advanced nations and to find its place in the European collective security system.

The fuel and energy sector is an essential component of the critical infrastructure. Particularly, the approved European Commission Directive 2008/114/EC[90] define energy as one of the two European critical infrastructure sectors. This sector containing eight subsectors: power industry (electrical grids and generating and transmission facilities; oil refining industry, oil extracting industry, oil pipelines and depots; gas producing industry, gas pipelines, liquefied gas terminals). Ensuring its sustainable functioning is one of the main tasks of any state.

Although the energy delivery system has changed since the 1970s, there is still a high risk of a supply disruption which could have great economic consequences. Capacity constraints have increased the potential of supply falling short of demand. Given this delicate balance of supply and demand, even a disruption of relatively small volume of oil, gas, coal

[90] Council Directive 2008/114/EC «On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection». – Retrieved from http://eur-lex.europa.eu/

can have a significant impact on the market. Global demand growth exacerbates market tightness, further re-enforcing the need for investment in capacity expansion. Geopolitical tensions and terrorism create uncertainty as to the continuous availability of supply. This «risk premium» adds to the volatility of an already tense market, where available energy supplies are increasingly concentrated in fewer countries. Natural disasters, such as extreme weather conditions, can disrupt the supply/demand balance, cutting off supply or causing demand to spike.

To counter these threats, EU member states are creating systems to respond to interruptions in the supply of energy. In particular, in accordance with EU Council Directive 2009/119/EC, they are required to have emergency reserves of crude oil and petroleum products.

In view of this, there is a need to implement the Directive 2009/119/EC is seen in Ukraine as one of the urgent tasks in the national security sphere.

UKRAINE'S COMMITMENTS AND ITS STATUS

The need to implement the requirements of Directive 2009/119/EC in Ukraine has been provided for by the Decision of the 10th Ministerial Council of the Energy Community of October 18, 2012[91]. The decision expands the sphere of application of the Treaty Establishing the Energy Community, which Ukraine joined on February 1, 2011[92].

A detailed plan of implementation of Directive 2009/119/EC in Ukraine was adopted on April 8, 2015[93] in order «to enhance the level of the state's energy security by establishing an efficient system of protection of the Ukrainian economy from sudden accidental and long-lasting termination of supply of oil and petroleum products caused by man-made, natural, military, political, and other crises in the oil-supplying countries»[94].

The main tasks of the Plan were identified as:

---

[91] Decision of the 10th Ministerial Council of the Energy Community. – Retrieved from http://www.energy-community.org/pls/portal/docs/1766216.pdf

[92] Treaty Establishing the Energy Community. – Retrieved from http://zakon3.rada.gov.ua/laws/show/994_a27

[93] See: http://zakon2.rada.gov.ua/laws/show/346–2015-p

[94] Plan of implementation of Directive 2009/119/EC. – Retrieved from http://www.kmu.gov.ua/document/248091904/Dir_2009_119.pdf

- development of legal, organizational, financial and economic principles for the establishment and functioning in Ukraine of a system of the minimum reserves of oil and petroleum products;
- regulation of relations in the sphere of minimum reserves management.

At the same time, it was stated that the system of the minimum reserves of oil and petroleum products in Ukraine should be based on a stage-by-stage development taking into account the principles of the EU legislation «of an extensive and modern network for efficient storage of oil, connected to refineries, export and import terminals as well as other infrastructure» that will exist «within the system of the main oil pipelines»[95].

Unfortunately, Ukraine still working to implement the majority of tasks related to the implementation of Directive 2009/119/EC despite the clear goals, developed plans, available support from the partners and establishment of several working groups.

Given this, Ukraine's priority should be to determine the model and approve the action plan for the creation of minimum oil and petroleum products stocks, as well as the adoption of normative acts necessary for their formation and the development of a management system for them.

The following questions still remain unanswered:

1. What are the «state», «emergency», «strategic», «stabilization», «crisis» reserves? What is the difference between them? What exactly should be stored and where? What is the purpose of the created reserves? Who will determine the efficiency of its creation and use and according to which criteria?

2. Under what conditions should the reserve be used? What are the risks related to storage, transportation, and use of the reserves under all possible scenarios? What is the difference in the need for oil and petroleum products in the event of occurrence of each scenario? What is the meaning of the phrase «inability of the ordinary channels to provide consumers with petroleum products»? Who will determine this and on what grounds?

3. Which companies will process crude oil and place it for storage? What is the procedure for its transportation, and how to assess the related risks? On what terms should oil be processed? Can the OPP owner

[95] See ref. 94

impose conditions of cooperation that are unprofitable for the state in the event of emergence of a crisis situation? How will the needs of the national economy be met during the period necessary for oil processing?

4. What will be the responsibility of the owners of petroleum depots for violation of storage agreements? What should be done in the case of bankruptcy of companies that stored the reserve oil and petroleum products?

5. What should be the procedure for reserves renewal? What will be the impact of availability of large volumes of petroleum products for free trade during the period of reserve renewal? What should their price be? What should be the procedure for their sale? Will the market participants be notified about the plans of procurement of new and sale of the renewed volumes of petroleum products? Will the replacement of reserves be reflected in the estimated balance sheet of the Ministry of Energy and Coal Industry?

Having received answers to the above questions, the public authorities responsible for implementing Directive 2009/119/EC will be able to approach the work more systematically. This will also be facilitated by the approval of the Energy Strategy of Ukraine until 2035, in which Ukraine's commitments to create energy reserve, which is necessary for the sustainable functioning of critical infrastructure, has been confirmed.

PROSPECTS FOR ESTABLISHING AN THE ENERGY RESERVE

It would be wrong to believe that the issue of reliable energy supply is reduced only to solving the problem of being dependent on imports and increasing the domestic extraction volumes. Increasing the reliability involves development and implementation of a vast range of initiatives aimed at diversifying generation and wider use of technologies that ensure the highest coefficients of energy transformation.

At the same time, it is Ukraine, which has the experience of hybrid war when the reserves in the Autonomous Republic of Crime, Donetsk and Luhansk were seized by the enemy, should present new initiatives in the sphere of guaranteeing collective energy security of Europe.

The respective vision should be based on the following theses:

- every consumer should have a possibility to use different sources of energy at different time;
- the energy consumption structure should be determined taking into consideration economic and environmental feasibility;

- fuel and energy production should be decentralized, and energy flows should be disaggregated;
- in every region, its own energy reserve should be created taking into account the energy consumption structure and various time of seasonal load, provided the state preserves its function to manage these reserves during the special period.

Such approach differs from the accepted EU policy on creating oil reserves. The problem is that the requirements concerning the 90-day reserve were formulated in the early 2000s when the oil prices were relatively low. At that time, the issues related to increasing energy efficiency and energy conservation were not yet so pressing. The transfer to renewable sources was not discussed, and climate change was debated upon exclusively by the academic community. However, after the increase of the oil prices and the EU accession of twelve new member states with limited financial possibilities for creating their own resources, the Union's plans began to cause doubts. In view of this, the new EU member states had to demand answers to the following *questions*:

- Why should the oil reserves be created and stored by every country, and not only by those countries that have such possibilities?
- Why should the volume of oil reserves of the EU member states suffice to cover precisely 90-day replacement of imports?
- Why is the volume of oil reserves estimated on the basis of consumption in an «ordinary» situation not taking into consideration the «emergency» (frenzy), seasonal and other factors?
- Why are the consumption volumes measured using tons, and not using the energy characteristics of the resource taking into consideration the predictable nature of its use and the role in guaranteeing energy security?
- What should be the threshold volumes of concentration of the reserve resources, and does such concentration increase environmental and other risks related to emergency situations?
- Why is mutual replace ability of energy resources not taken into consideration?
- Is it possible to create the strategic reserve by reserving the facilities for production of necessary energy commodities and feedstock?
- Is it possible instead of the oil reserve to create a reserve system that would combine the reserves of various types of fuel and ensure

sustainable functioning of all branches of economy, and not only its transport component?

In the event of a positive answer to the last question, it will be possible to develop the requirements for the system of collective energy security based on creation of the reserves of facilities in the sphere of oil processing, coal, oil and gas industry, nuclear, renewable energy and electricity taking into consideration the possibility of a rapid change of the structure of consumed energy resources. In this process, in order to decrease the impact of the price component on the functioning of this system, a mechanism of financial risks hedging should be developed as well.

Such approach will make it possible to mitigate the outcomes of the growth of prices for energy resources and the increased volumes of their consumption and by this increasing resilience of energy sector.

EARMARKED STATUS OF RESERVES UNTIL 2035

The reserves of oil and petroleum products have to be created for the 90-day period of consumption in normal demand conditions. Since this is a time-consuming and costly process, it is recommended that the reserves should be created on a stage-by-stage basis, simultaneously with the development of the respective financing mechanisms.

Since the structure of oil reserves should provide for the possibility of prompt response to a rapidly changing situation, it is not feasible to create the reserve of domestically produced feedstock (in the volume totaling 25 % of its annual consumption) during the first stage of creation of the minimum reserves.

The priority task should be to create the motor fuel reserve in the volume totaling 20-day period of consumption in normal demand conditions.

The structure of such reserve should correspond to the structure of sales of light petroleum products for cash.

For the period ending 2025, further increase of the volumes of reserves should be envisaged for each company working in this market – up to 10 % of the annual sales volume. Starting 2021, simultaneously with the creation of the reserves of oil and petroleum products, there should be a transfer to creation of flexible energy reserve since the availability of oil reserves only, as they are currently understood, will

result in creation of an inefficient structure from the energy security point of view.

In addition:

- the structure of energy reserves in Ukraine should comply with the structure of energy consumption, combine the reserves of various types of fuel and energy, and ensure sustainable functioning of all branches of economy, and not only transport (such as oil and petroleum products);
- every consumer should have a possibility to use various sources at various time, while the structure of energy consumption at a local level should be determined taking into consideration economic and environmental feasibility;
- production of fuel and energy should be decentralized;
- reserves of fuel and energy should be created in every region, provided the state preserves its function to manage these reserves during the special period, and energy consumption structure as well as various time of seasonal load is taken into account;
- energy flows should be disaggregated.

The optimization objective can be formulated as follows:

- restriction – the identified level of energy security that takes into consideration the structure of regional energy supply and energy consumption; time lines for the country's achieving the identified security level;
- the target function – the cost of the project that will be determined on a stage-by-stage basis but minimized for the project in general.

Such an author's approach to the development of tools to ensure the stability of the functioning of the energy sector differs from the model that Ukraine is supposed to implement according to obligation and is proposed for discussion. At the same time, this approach calls for extensive involvement of private enterprises in the creation of flexible energy reserve. Thus, the task of forming the stability of the state will be fulfilled not only by state authorities, but also by the public.

It is suggested that the flexible energy reserve and, in particular, the oil reserve in Ukraine should be created using a mixed private-public model, according to which the reserves are managed by a special agency (association), whose members are market participants and representatives of governmental bodies.

Forming and development of the state-private partnership are critical for the public policy on critical infrastructure protection and it should

be regulated by the law, should find methodological, organizational and technical support for coordinated actions. Besides, mutual relations between private enterprises and the state, both in supporting energy reserve system functioning and in exchanging information as per the stipulated requirements will demand regulatory, organizational and technical arrangements in the scope of the state critical infrastructure protection system operation.

During the preparation of regulatory and legal provisions it is necessary to take into account that the components of a flexible energy reserve can be the following:

- insurance reserves of natural gas in the amount of 10 % of the planned monthly volumes of supply to consumers that will be created by its suppliers for their own or raised funds (as established by the Cabinet of Ministers Decree No. 860 dated November 16, 2016)[96];
- irreducible coal reserves in the total amount of at least 5 million tons that must be created at each thermal power plant and coal handling preparation plants that use this type of fuel, as well as in enterprises that use coal as raw materials and in the state reserve (currently the State Agency for Reserve of Ukraine does not have coal reserves, although this type of fuel is present in the storage classification).

To this end it is *recommended* that:

1. The applicable legislation should be complemented with normative legal acts that would regulate organizational and economic principles of creation and management of energy reserves, including development of mechanisms and conditions for its creation, storage, release (use) and renewal.

2. An institutional structure should be established for management of the energy resources, which process includes:

- creation of a management body that within the framework of its terms of reference will establish the reserve structure and manage it;
- involvement of participants of the energy products market in the process of creation of the reserve;
- development of the rules of procedure regulating work of all participants of creation, maintenance, and functioning of the reserves;

[96] Decree of the Cabinet of Ministers of Ukraine of 16 November 2016 № 860. – Retrieved from http://zakon3.rada.gov.ua/laws/show/860–2016-%D0 %BF

- separation of the created reserves from the state reserves for the special period, state reserve stock, stabilization reserves, and other special-purpose reserves of the country.

3. A system for publishing information about creation, storage, release (use), and renewal of the energy reserve should be developed.

4. The infrastructure of energy reserve should be created taken into consideration the needs of the regions as well as the reservoir fleet available in their territory.

The principal mechanisms of financing creation of energy reserves in Ukraine should be:

- purchase of energy products with the funds received as a result of increasing taxes for fuel. At the same time, one should explain to the citizens of Ukraine the need for this step and at a legislative level ensure the earmarked use of these funds for creation of the reserves;
- the reserve agreements that provide for a possibility to buy out the reserves owned by other companies at any time for the market prices. Respective services are provided to the agencies that do not have sufficient reserves by international banks, among others, by Goldman Sachs, at 2…3 %[97].

The formation of a flexible energy reserve, which will consist of various types of fuel and energy, will ensure the sustainable functioning of all sectors of the economy, and not just transportation (as provided by the oil reserve), and will be a step towards the increasing resilience of Ukrainian energy sector.

[97] Such offer was already received by National Joint Stock Company *Naftogaz of Ukraine* in May 2012.

3.5. IMPLEMENTATION OF DISASTER RISK REDUCTION APPROACH FOR CRITICAL INFRASTRUCTURE PROTECTION IN UKRAINE

Awareness of the global trend towards the proliferation of negative natural and man-made processes, increasing the magnitude of their negative effects and losses, significantly updated for Ukraine the necessity of protection of systems, objects and resources vital for society, socio-economic development of the country and ensuring national security. Proceeding from the needs of national security and the requirement to introduce a systemic approach to solving the problem of CIP at the national level, the creation of a CIP system is one of the current priorities in reforming the security and defense sector of Ukraine. At present, the lack of unified methodology for assessing threats and risks of natural and man-made origin for CI, preventing their implementation and responding to them is among the pressing problems in the field of building a state system for the CIP.

The operation of numerous mining, chemical, energy companies, a large number of industrial and urban agglomerations with the high population density determine the increase of emergencies with large negative consequences due to the threat of damage and destruction of CI objects. Among such objects specially threatened are spatially distributed railways, oil and gas pipelines, bridges, potentially hazardous production, main electrical grids, whose safe operation is of paramount importance for the socio-economic development of Ukraine.

In line with recent UN data, more than 700 thousand people have lost their lives, over 1.4 million have been injured and approximately 23 million have been made homeless as a result of disasters over the

past 10 years[98]. Overall, more than 1.5 billion people have been affected by disasters in various ways in vulnerable situations disproportionately affected. Total economic loss was more than $1.3 trillion. In addition, between 2008 and 2012, 144 million people were displaced by disasters.

Disaster can be defined as a serious disruption of the functioning of a society involving widespread human, material, economic or environmental losses and impacts, which exceeds the ability of the affected society to cope using its own resources[99]. Disasters could be described as a result of the combination of the exposure to a hazard, the conditions of vulnerability that are present and insufficient measures to reduce or cope with the potential negative consequences. Disaster impacts may include loss of life, injury, and disease and other negative effects on human well-being, damage to critical infrastructure, destruction of assets, loss of services, social and economic disruption and environmental degradation.

Because many disasters are intensified by climate change and are increasing in intensity, CI becomes vulnerable to their devastating effects. Various evidences indicate that exposure of persons and critical infrastructure in many countries has been increased faster than vulnerability has decreased, thus generating new risks and a steady rise in disaster-related losses, with a significant economic, social, health, cultural and environmental impact at the local and state levels. All countries especially developing ones, where the mortality and economic losses from disasters are excessively higher, are faced with increasing levels of possible hidden costs and challenges in order to protect population and CI.

In current conditions it is urgent to anticipate plan for and reduce disaster risk in order to more effectively protect people, communities and countries, their livelihoods, health, CI and ecosystems, and strengthen their resilience in the face of various threats of natural and made-man origin. Disaster risk reduction (DRR) is the concept and practice of reducing disaster risks through systematic efforts to analyse and manage the causal factors of disasters, including through reduced exposure to hazards, lessened vulnerability of people and CI, wise

[98] Sendai Framework for Disaster Risk Reduction 2015–2030. – Retrieved from http://www.unisdr.org

[99] United Nations Office for Disaster Risk Reduction (UNISDR), «2009 UNISDR Terminology on Disaster Risk Reduction», Geneva, May 2009. – Retrieved from http://www.unisdr.org/we/inform/terminology

management of land and the environment, and improved preparedness for adverse events.

Considering threats of industrial origin, it should be noted that in Ukraine because of the high level of depreciation of fixed assets there is a risk of accidents at CI objects, especially at the power facilities and life-support networks. According to the information of the SESU Ukraine accidents at 955 objects included into the State Register of Increased Danger Objects may lead to emergency situations of the national or regional level, which may also threat CI, specifically in terms of operation of fuel and energy complex facilities, bridges and roads, utility infrastructure[100].

According to the experts of the German reinsurance company Munich Re there were 336 disaster events in 2014, among them the natural catastrophes have reached the highest level ever recorded in one year at 189 events while 147 were man-made disasters. More than 12700 people lost their lives or went missing because of these events. Estimated total economic losses from natural catastrophes and man-made disasters were USD 110 billion in 2014, down from USD 138 billion in 2013. At the same time losses from natural disasters were around USD 101 billion in 2014 originating mostly by floods, tropical cyclones and severe convective storms in Asia, North America and Europe[101].

Ukraine is not an exception from global trends. Today in Ukraine there are a lot of emergency situations of natural and man-made origin. These scale negative consequences of these events are becoming more dangerous for people, environment and CI.

Among these types of threats it is worth distinguishing meteorological ones which frequency has increased significantly in recent decades, in particular ice, flooding, droughts. Among the hydrological threats the most serious consequences for CI have floods. In particular, the biggest flood in recent years in Ukraine in 2008 caused damage to more than 500 highway bridges, erosion of 1660 km of roads of different types.

---

[100] The Role of Hydrometeorological Services in Disaster Risk Management. Proceedings from the joint workshop co-organized by: the World Bank, the United Nations International Strategy for Disaster Reduction, and the World Meteorological Organization. Washington, D.C. – March 12, 2012.

[101] Natural catastrophes and man-made disasters in 2014. – Retrieved from http://www.munichre.com

Significant threat to the operation and security of CI are dangerous exogenous geological processes including flooding, subsidence, karst and landslides. Activation of dangerous exogenous processes threatens environmental security and CI in areas where increased danger objects are situated. Among them most vulnerable are protective dikes, dams of slime storage, sumps, complications of geological and technical conditions of operation of industrial facilities and engineering networks of industrialized urban agglomerations.

The analysis showed an increase in the threat of reducing the level of safety of numerous CI objects in Ukraine as a result of overtime exploitation of structures, structures, equipment and engineering networks operating on the verge of exhaustion of their resource and forms a serious risk of emergencies of natural and man-made nature for the safety of operation CI.

It should also be borne in mind that due to global climate change in the list of major threats in the near future will dominate the meteorological events. The UN estimates that in the future on the most territory of Europe there will be significant increase of the frequency of flooding: from once per 100 years up to one event for 5–15 years. Regarding Ukraine may be noted that the catastrophic consequences of floods in 2001, 2008 and 2010 in the western regions of the state once again demonstrated the need for measures to reduce the risks of natural disasters of hydro meteorological origin. Attention must be drawn to the fact that economic losses resulting from natural disasters far exceed losses from man-made ones.

All together the amount of losses from natural and made-disasters in Ukraine has been fluctuating during the last 5 years from 1 billion UAH in 2010 to 190 million UAH in 2014[102].

This situation, together with the increasing vulnerability of the population because of demographic, technological and socio-economic transformations taking place in terms of the spread of urbanization, environmental degradation, and global climate change can lead to the fact that in the near future accidents and natural disasters will constitute a greater threat to the economy, population and CI.

---

[102] National Report on the State of Technological and Natural Safety in Ukraine in 2013. – Retrieved from http://www.dsns.gov.ua/files/prognoz/report/2013/%D0%A1%D0%90%D0%99%D0%A2_%D0%94%D0%A1%D0%9D%D0%A1.rar

It is now clear that more dedicated actions need to be focused on tackling the consequences of climate change and variability, unplanned and rapid urbanization, insufficient land management and compounding factors such as demographic change. In this regard special attention should paid to addressing the lack of regulation and incentives for private disaster risk reduction investment, complex supply chains, limited availability of technology, unsustainable uses of natural resources as well as declining ecosystems. Moreover, it is necessary to continue strengthening good governance in disaster risk reduction strategies at the national, regional and global levels and improving preparedness and national coordination for disaster response, rehabilitation and reconstruction.

1. The international approach to disaster risk reduction

Nowadays at international level widely recognized that targeted efforts to reduce the risk of natural and man-made disasters should be systematically integrated into policies, plans and programs for sustainable development and critical infrastructure protection under conditions of enhanced regional and international cooperation in this area. UN documents on sustainable development, poverty reduction, good governance and disaster risk reduction are interdependent and related tasks, so it efficiently in the future needs to intensify efforts to create regional and national levels prerequisites to reduce this risk. Such approach has been recognized by many countries as an important component for achieving the internationally agreed objectives of sustainable development in accordance with the objectives of the Millennium Declaration[103].

The importance of coordinating the efforts of disaster risk reduction at the international, regional and national levels in recent years emphasized in a number of multilateral framework programs and declarations. Among these, the most important is «Yokohama Strategy and Plan of Action for a Safer World. Guidelines for Natural Disaster Prevention, Preparedness and Mitigation» which was adopted in 1994[104].

---

[103] United Nations Millennium Declaration. Resolution adopted by the General Assembly. – UN, 2000. – Retrieved from http://www.un.org/millennium/declaration/ares552e.htm

[104] International Decade for Natural Disasters Reduction. Yokohama Strategy and Plan of Action for a safer world. In: World conference on natural disaster reduction, Yokohama, Japan, 1994. – Retrieved from https://www.unisdr.org/we/inform/publications/8241

At the World Conference on disaster risk reduction (2005), representatives of the governments of 168 countries, including Ukraine, have adopted Hyogo Framework for Action (HFA) in 2005–2015: «Building the Resilience of Nations and Communities to Disasters». They did it to support the establishment and strengthening of national integrated mechanisms such as multi-national platform and give priority to measures to reduce disaster risk at national and local levels. The concept of «national platform for disaster risk reduction» is defined as a certain mechanism in the form of a forum or committee with stakeholders that promotes disaster risk reduction measures at different levels and provides coordination efforts, analyse information and make recommendations on priority areas that require coordinated activities[105].

Since the adoption of the Hyogo Framework for Action in 2005 the progress has been achieved in reducing disaster risk at local, national, regional and global levels, leading to a decrease in mortality in the case of some hazards. International mechanisms for strategic coordination and partnership development for disaster risk reduction, such as the Global Platform for Disaster Risk Reduction and the regional platforms for disaster risk reduction, as well as other relevant international and regional forums for cooperation, have been instrumental in the development of policies and strategies and the advancement of knowledge and mutual learning.

As a result the Sendai Framework for Disaster Risk Reduction 2015–2030 was adopted at the Third United Nations World Conference on Disaster Risk Reduction, held on 14–18 March 2015 in Sendai, Miyagi, Japan. During the Conference, States reiterated their commitment to address disaster risk reduction and the building of resilience to disasters with a renewed sense of urgency within the context of sustainable development and poverty eradication, and to integrate, as appropriate, both disaster risk reduction and the building of resilience into policies, plans, programmes and budgets at all levels and to consider both within relevant frameworks.

The Sendai Framework for Disaster Risk Reduction aims to achieve the substantial reduction of disaster risk and losses in lives, livelihoods

[105] Hyogo framework for action 2005–2015: building the resilience of nations and communities to disasters. In: World conference on disaster reduction, Kobe, Japan, January 2005. – Retrieved from http://www.unisdr.org/we/inform/publications/1037

and health and in the economic, physical, social, cultural and environmental assets of persons, businesses, communities and countries over the next 15 years. Successful achievement of this outcome will be subject to the realisation of the main goal that comprises the prevention of new and reduction of existing disaster risk through the implementation of integrated and inclusive economic, structural, legal, social, health, cultural, educational, environmental, technological, political and institutional measures that prevent and reduce hazard exposure and vulnerability to disaster, increase preparedness for response and recovery, and thus strengthen resilience.

To support the assessment of global progress in achieving the outcome and goal of the Sendai Framework, the following seven global targets have been agreed:

1) reduce global disaster mortality by 2030, aiming to lower the average per 100,000 global mortality rates in the decade 2020–2030 compared to the period 2005–2015;

2) reduce the number of affected people globally by 2030, aiming to lower the average global figure per 100,000 in the decade 2020–2030 compared to the period 2005–2015;

3) reduce direct disaster economic loss in relation to global gross domestic product by 2030;

4) reduce disaster damage to critical infrastructure and disruption of basic services, among them health and educational facilities, including through developing their resilience by 2030;

5) increase the number of countries with national and local disaster risk reduction strategies by 2020;

6) enhance international cooperation to developing countries through adequate and sustainable support to complement their national actions for implementation of the present Framework by 2030;

7) increase the availability of and access to multi-hazard early warning systems and disaster risk information and assessments to people by 2030.

Taking into account the expected outcome of Sendai Framework, there is a need for focused action across various sectors by States at local, national, regional and global levels in the priority areas including understanding disaster risk, strengthening disaster risk governance to manage disaster risk, investing in disaster risk reduction for resilience, enhancing disaster preparedness for effective response and recovery, rehabilitation and reconstruction activities related to CIP.

Policies and practices for disaster risk management should be based on understanding of disaster risk in all its dimensions of vulnerability, capacity, exposure of persons and assets, hazard characteristics and the environment. Such knowledge can be leveraged for the purpose of pre-disaster risk assessment, for prevention and mitigation and for the development and implementation of appropriate preparedness and effective response to disasters.

Disaster risk governance at the national, regional and global levels is of great importance for an effective and efficient management of disaster risk. Clear vision, plans, competence, guidance and coordination within and across sectors, as well as participation of relevant stakeholders, are needed. Strengthening disaster risk governance for prevention, mitigation, preparedness, response, recovery and rehabilitation is therefore necessary and fosters collaboration and partnership across mechanisms and institutions for the implementation of instruments relevant to disaster risk reduction in the field of sustainable development and CIP.

One of the priorities of the Sendai Framework for Disaster Risk Reduction is public and private investment in disaster risk prevention and reduction through structural and non-structural measures. They are essential to enhance the resilience of population, critical infrastructure and environment. Such measures are cost-effective and instrumental to save lives, prevent and reduce losses and ensure effective recovery and rehabilitation.

The steady growth of disaster risk, including the increase of people and assets exposure, combined with the lessons learned from past disasters, indicates the need to further strengthen disaster preparedness for response, take action in anticipation of events, integrate disaster risk reduction in response preparedness and ensure that capacities are in place for effective response and recovery at all levels. Various disasters have already demonstrated that the recovery, rehabilitation and reconstruction phase, which needs to be prepared ahead of a disaster, is a critical opportunity to «Build Back Better», including through integrating disaster risk reduction into development measures, making nations and communities resilient to disasters.

International cooperation for disaster risk reduction is a critical element in supporting the efforts of developing countries to reduce disaster risk. In addressing economic disparity and disparity in

technological innovation and research capacity among countries, it is crucial to enhance technology transfer, involving a process of enabling and facilitating flows of skill, knowledge, know-how and technology from developed to developing countries in the implementation of the present Framework.

In this connection it is very important to enhance access of developing countries to finance, environmentally sound technology, science and inclusive innovation, as well as knowledge and information-sharing through existing mechanisms, namely bilateral, regional and multilateral collaborative arrangements, including the United Nations and other relevant bodies.

2. Disaster risk reduction in Ukraine

Despite formal involvement of Ukraine in HFA and positive experience of national platforms in most EU and CIS countries, Ukraine has not established such a mechanism yet. As for neighboring European countries, the national platform is already functioning in Poland, Hungary and Turkey. At the same time, the most part of European national platforms for DRR (18) has the status of public institution, and only three of them operate as NGOs.

However in view of the signing of the Association Agreement between the EU and Ukraine (AA) in 2014 the importance of DRR approach in Ukraine has been recognized as one of the priorities for implementation. According to the AA the rule of law, good governance, the fight against corruption, the fight against the different forms of trans-national organized crime and terrorism, the promotion of sustainable development and effective multilateralism are central to enhancing the relationship between the EU and Ukraine.

Ukraine recognizes the value of international environmental governance and agreements as a response of the international community to global or regional environmental problems. The Parties reaffirm their commitment to the effective implementation in their laws and practices of the multilateral environmental agreements to which they are party.

The DRR approach is considered of great importance taking into account its orientation to the preventive of negative consequences. It is very important to cooperate in order to promote the rational utilization

of natural resources in accordance with the objective of sustainable development with a view to strengthening the links between the EU and Ukraine on critical infrastructure protection issues, environmental policies and practices.

Cooperation in the civil protection sector shall take place through the implementation of specific agreements. It shall aim at facilitating mutual assistance in case of emergencies, assessment of the environmental impact of disasters, critical infrastructure protection, strengthening existing cooperation on the most effective use of available civil protection capabilities.

In 2009 between the SESU and United Nations Development Programme a Memorandum of Understanding on cooperation in the field of natural risk reduction and rapid recovery has been signed. Thus, the government of Ukraine has received certain obligations to take measures to reduce disasters risks and reduce the impact of potential threats to social and economic welfare.

The memorandum notes that global contributions to DRR is a prerequisite for achieving the Millennium Development Goals, particularly in sustainable development and poverty reduction, and that the question of DRR involved in the global strategic plan of UNDP for 2008–2011. Ukraine recognizes the need to expand existing approaches to disaster response, focusing on issues of improving preparedness and risk reduction, as well as working towards the development of the Action Plan with the objectives of HFA. The document stated that the issue of risk reduction and adaptation to global climate change by reducing the impact of prevention and mitigation of threats, preventing the loss or damage because of meteorological and man-made disasters are important elements of sustainable development.

Obviously, the SESU should be the lead agency in Ukraine to create a national platform for DRR. The representatives of the NSDCU, the NISS, the State Agency of forest resources, the State Water Resources Agency, as well as specialists in the regions of Ukraine that are most affected by natural disasters and man-made ones must be involved in this mechanism as well as international organizations.

After its creation, the national platform will coordinate the efforts in the field of disaster risk reduction, and mobilize the resources of private companies and international organizations. Generally, this will allow effectively allocate all of the available resources for protection and

concentrate efforts in terms of time limits in accidents of various origin which are threatening CI.

International experience shows that creation of a national platform for DRR in Ukraine will have a number of benefits. Among them is the ensuring coordination of efforts to reduce the risks of disasters, resource mobilization of private companies and international organizations, exchange of experience with experts in the field of DRR from around the world.

In current conditions, there is tangible tendency towards further reduction of the level of safety and reduction of the duration of operation of objects of CI due to overtime operation of structures, structures, equipment and engineering networks which operate on the brink of exhaustion of their resources and initiate serious threats of emergencies of natural and man-made nature for the safety of the operation of CI objects.

Development and implementation of DRR approach for CI objects is hampered by the lack of a national body responsible for coordinating the existing state security and crisis response systems in the field of CIP at the national level.

The legal framework in the country does not fully take into account the positive foreign experience as well as the main provisions of international instruments in the field of DRR with regard to CIP. There is also very important to provide full participation of relevant CI stakeholders at appropriate levels in the DRR process, to invest in the economic, social, health, cultural and educational resilience of persons, communities, countries and the environment through technology and research, enhancing multi-hazard early warning systems, preparedness, response, recovery, rehabilitation and reconstruction.

Ukrainian needs to enhance the scientific and technical work on DRR and its utilization through the coordination of various networks and scientific research institutions with the support of the United Nations Office for Disaster Risk Reduction Scientific and Technical Advisory Group, in order to strengthen the evidence-base in support of the implementation of the Sendai Framework for Disaster Risk Reduction.

Prospects for further developments in this area are related to conducting an assessment of the risks of emergence of natural and man-made disasters for CI objects of Ukraine, their categorization by types and levels of risk, as well as the development of well-grounded measures to

prevent the emergencies with large negative consequences for critical infrastructure objects.

Important for the risk assessment is an availability of operational and objective data on monitoring of actual natural and man-made threats, especially regarding economic losses from their implementation. This information should be provided annually by the Ministry of Ecology and Natural Resources and the SESU in the form of reports on the state of the environment and the state of man-made and natural safety, respectively. In this regard, the restoration of proper functioning of the Government information and analytical system for emergencies and the improvement of early detection of threats on the basis of this system as well as risk reduction of emergencies of natural and man-made nature on CI objects is essential.

SUMMARY

For stable and safe existence, a contemporary society and its members should sustainably receive a number of various products and services, should have access to a number of critical resources, etc. For this purpose, a number of assets, networks and systems, both physical and virtual, are created and operated. The most important of them are assigned to national critical infrastructure. This national critical infrastructure stipulates state's resilience and its capacity to confront internal and external threats and to respond adequately to modern challenges.

Destruction, breakdowns of national critical infrastructure, formation of failures and essential limitations in providing vital services and access to critical resources cause serious impacts for health and well-being of public, sustainable and successful society and national economy functioning, threaten national security and the existence of a State.

Therefore, enhancing of critical infrastructure protection and resilience has become a priority of national security policy in many countries. World best practice demonstrate the need to build critical infrastructure protection system capable to prevent, mitigate and respond to all types of threats (i. e. natural, man-made, criminal and terrorist threats) and their possible combinations.

The hybrid war against Ukraine have gave an additional impetus to establish a state system on critical infrastructure protection, taking into account the fact that the aggressor state can use terrorist and criminal acts as one of the tools of the hybrid warfare.

Necessity to be prepared to withstand such threats and their combinations raises acutely the issues of information exchange, interaction and coordination, utilization of all available resources to confront threats to critical infrastructure. Though there is a range of laws and regulations that define authority and competence of government agencies in

this sector and associated sectors, Ukraine still lacks a nation-wide systematic approach to management of protection and security of the whole aggregate of such systems, objects and resources, considering mutual interface between some objects customarily attributed to critical infrastructure.

The tasks of enhancing security and resilience of CIP cannot be achieved within existing systems designed to provide separately civil protection system, counter-terrorism protection, cyber threat counteraction etc. and demand legal, institutional and organizational novelties. There is an urgent need to involve all stakeholders (operators, regulators, local executive authorities, public etc.) in the activity aiming at considerable improvement of state critical infrastructure security and resilience against all threats and hazards.

Specification of CIP system's tasks requires further discussion and development of relevant legislation. Establishment of a state CIP system requires legislatively defining its fundamental principles of operation, application of common approaches to management of CI security at all levels, clear identification of the principles of interaction and cooperation among state authorities, private business, society and public.

Improvement of the national legislative and normative basis for CIP shall be based on unified approaches, a single methodological and terminological basis recognized by all parties involved in state the CIP system operation. To facilitate achievement of this purpose the Concept defines the Bearing in mind the strategic role of Ukraine in terms of global security we expect that our country's efforts in this field will be supported by the leading nations in the world. Cooperation with international experts contributes to creation of a "critical mass" of the Ukrainian public servants, scholars, experts needed to provide necessary decisions. The breakthrough decision of the National Security and Defense Council of Ukraine «On improvement of measures to ensure the protection of critical infrastructure objects» enacted by the Presidential decree, was prepared with participation of the Ukrainian and European experts and became one of the examples of successful cooperative efforts.

We strongly hope that NISS expert's research results presented in this book will make a due contribution to Ukraine's progress on its way to a sovereign, secure and resilient State.

Наукове видання

РОЗВИТОК СИСТЕМИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ

Монографія
(англійською мовою)

Це видання представляє багаторічну роботу експертів та науковців Національного інституту стратегічних досліджень (у галузі досліджень проблем забезпечення енергетичної та техногенної безпеки) щодо впровадження в Україні найкращих світових політик і практик у сфері захисту національної критичної інфраструктури. У виданні узагальнено результати досліджень, подано базові законодавчі та концептуальні документи, аналітичні та оглядові матеріали, присвячені питанням упровадження концепції захисту критичної інфраструктури в Україні.

Це перше англомовне видання, у якому висвітлюються стан досягнутого прогресу і проблеми, які Україна має вирішити, щоб забезпечити відповідність рівня захисту та стійкості критично важливої інфраструктури відповідно до сучасних викликів та загроз.

Для іноземних партнерів, котрі співпрацюють з Україною у сферах національної безпеки, захисту критичної інфраструктури, врегулювання кризових ситуацій тощо. Книга також буде корисною представникам органів державної влади України, правоохоронних та розвідувальних органів, державних і приватних компаній, ученим, експертам і всім, хто цікавиться темою захисту та відтворення критично важливої національної інфраструктури та пов'язаних з нею питань.

В авторській редакції

Коректура: *Т.В. Карбовнича, О.М. Романова*
Комп'ютерне верстання: *О.М. Адулов*
Оформлення обкладинки,
відповідальний за випуск: *О.М. Романова*

Оригінал-макет підготовлено
у Національному інституті стратегічних досліджень:
вул. Пирогова, 7-а, Київ-30, 01030
Тел./факс: (044) 234–50–07
e-mail: info-niss@niss.gov.ua

Формат 60х84/8. Ум. друк. арк. 21,39.
Наклад 300 прим. Зам. № ДФ __

ПП «Видавництво Фенікс»
Свідоцтво суб'єкта видавничої справи
ДК № 271 від 07.12.2000 р.
03067, Київ, вул. Шутова, 13-б
www.fenixprint.com.ua

ДЛЯ НОТАТОК

ДЛЯ НОТАТОК