THE NATIONAL INSTITUTE FOR STRATEGIC STUDIES

GREEN PAPER
ON CRITICAL INFRASTRUCTURE PROTECTION IN UKRAINE

Analytical Report

Kyiv – 2015

UDC 354+321+355+327

Authors:
D. Biriukov, Candidate of Technical Sciences,
S. Kondratov,
O. Nasvit,
O. Sukhodolia, Doctor of Public Administration, Professor

General editor O. Sukhodolia, Doctor of Public Administration, Professor

Electronic version: http://www.niss.gov.ua
Green Paper for the Protection of Critical Infrastructure in Ukraine: Analytical Report / D. Biriukov, S. Kondratov, O. Nasvit, O. Sukhodolia. - Kyiv. : NISS, 2015. – 33 pages.

This Green Paper raises issues related to the establishment of a critical infrastructure protection system in Ukraine. It formulates strategic objectives of the public policy in the area of critical infrastructure protection in Ukraine, principles for the establishment of a critical infrastructure protection system and tasks for this system. Prior steps toward establishment of a state-level critical infrastructure system in Ukraine are formulated. These were drawn based on the analysis of experience of EU and NATO member states, contemporary security environment in Ukraine, and the priorities of the national security and defense sector reform.

The Green Paper has been developed to fulfill the task of the Annual National Program of Ukraine-NATO Cooperation (2015).

Foreword

Preparation and publication of "green papers" is a widespread practice to stimulate and organize professional discussion of topical security subjects and ways to address them both nationally and internationally. As a rule, publication of a "green paper" precedes the subsequent stage: development and publication of an official paper formulating essentials of the government policy to address the defined problem. This Green Paper reviews the issues of critical infrastructure protection in Ukraine – the area being a priority part of assurance of national security of the EU and NATO member states, as well as an component of the EU security policy at the pan-European level.

No doubt, global security developments seen in the world in the past two decades involve numerous crises of varied origins and nature. This indicates the shrinkage of forecasting horizon or even total lack of forecasting capability in the contemporary security management mechanisms, their inability to prevent low-probability emergencies of sophisticated nature, such as US terrorist attacks of 9/11, Hurricane Katrina in the US (2005), world financial crisis (2008), destructive earthquake and tsunami causing a Fukushima Daiichi Nuclear Power Plant accident in Japan (2011), events of the Arab Spring (2011), Russia's hybrid war against Ukraine, or this year's refugee crisis in the EU. Analysis of these, as well as the other large-scale and comprehensive challenges to regional and global security, as well as lessons learned from them clearly put on the agenda the need to assure protection of objects, systems and resources critical for the existence of the state (the critical infrastructure) against all types of threats and their combinations.

Protection of critical infrastructure as a security target emerged during the Cold War and became an actively developing trend in the leading countries in the beginning of this century in response to abrupt growth of a terrorist threat. This security area is seen as a priority by such international structures as the EU and NATO since, in addition to obvious benefits and advantages, globalization and IT development increase economic, financial, technological and resource interfaces and interdependences between different countries and their alliances, as well as between world regions, making modern society highly vulnerable to threats – in particular those targeting the nodal points of the described interfaces.

Realization of the growing terrorist threats in Europe caused the European Commission to develop and, in November 2005, publish the *Green Paper on the European Programme for Critical Infrastructure Protection*[1], and subsequently, in 2006, on completion of the consultations between the EU countries, the *European Programme for Critical Infrastructure Protection*[2]. Character of the EU approach specific for a community of independent states was reflected in the EC document entitled *Protecting Europe's Critical Energy and Transport Infrastructure* (February 2007)[3] and in a special directive for the identification of critical infrastructure objects and assessment of a need to enhance their protection (December 2008)[4]. Protection of critical power supply infrastructure was named a priority focus for the assurance of energy security of NATO member states and the Alliance in general in the Declaration of the Chicago Summit (20 May 2012).

Dramatic events of 2014-2015 in Ukraine increased urgency of protection of infrastructure, objects and systems vital for the activity of the society and created a need to establish a critical infrastructure protection system for Ukraine. We believe that harmonization of approaches for its establishment with those actively implemented by the EU and NATO will facilitate improvement of national security mechanisms and enhance capabilities of our state regarding integration in the European security context. Bifurcate nature 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 whose revision is currently underway.

In this light, using the green paper preparation experience of the EU and NATO member states, the National Institute for Strategic Studies (NISS) has initiated development of a draft Green Paper for Critical Infrastructure Protection in Ukraine.

The Green Paper for Critical Infrastructure Protection in Ukraine was developed with the support of the NATO Liaison Office in Ukraine as part of the Ukraine-NATO 2014 and 2015

Annual National Cooperation Programs. Work on the Green Paper was completed by NISS with the active involvement of Ukrainian and international experts.

Inter alia, preparation of the draft Green Paper built on the results of work of the Interagency Expert Working Group for the Suppression of Threat of Proliferation of Mass Destruction Weapons and Materials and Associated Terrorist Threats and Protection of Infrastructure Critical for State Activity (IEWG), established within the National Institute for Strategic Studies (NISS) in 2011, the analytical report prepared by NISS[i], as well as conclusions and recommendations of the July 2012 round table on this subject and the international scientific and practical conference Critical Infrastructure Protection Concept: State, Problems and Prospects of Implementation in Ukraine (November 2013) organized by NISS jointly with the NATO Liaison Office in Ukraine and PJSC Ukrhydroenergo.

We have taken into account numerous inputs from Ukrainian and international experts. We express gratitude for active participation in the work on individual Green Paper sections to Ukrainian experts: V. Bilokon, V. Grechaninov, O. Ievdin, V. Zaslavsky, V. Luchkov, M. Sungurovsky, O. Fal and to international experts: Valeri Ratchev and Todor Tagarev (Geneva Centre for the Democratic Control of Armed Forces), Krzysztof Brzozowski (Governmental Center for Security, Poland), Martin Linhart (NATO Liaison Office in Ukraine), Christian Papsthart (Federal Ministry of Interior, Germany), Monika John-Koch (Federal Office of Civil Protection and Disaster Assistance, Germany), Heiki Jakson (NATO Energy Security Centre of Excellence).

Discussion of Green Paper text with experts and consideration of suggestions received from concerned government agencies, companies, and research institutions allowed NISS to present this final version of the Green Paper for Critical Infrastructure Protection in Ukraine at the international expert meeting on 15-16 October 2015.

[i] D. Biriukov, S. Kondratov. Critical Infrastructure Protection: Problems and Prospects of Implementation in Ukraine (in Ukrainian). -K.: NISS, 2012. - 57 pages

Contents

1. 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 critical infrastructure 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 critical infrastructure at the time of peace is associated with the sustaining of vital functions of 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 critical infrastructure operation.

Implementation of such a mechanism would require profound survey of existing practice for critical infrastructure protection in Ukraine, currently dominated by departmental approaches, as well as analysis of interface 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.

2. 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.

2.1. 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 critical infrastructure 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."* (Patriot Act, 2001).

In Germany, critical infrastructure 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 critical infrastructure 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 critical infrastructure 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 critical infrastructure. It is functions and services provided to the society, business and the state by critical infrastructure assets and systems that are used as the basis for the definition of their criticality, which provides effective methodology for setting critical infrastructure element selection criteria and protection priorities[ii].

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 critical infrastructure definition. For the first time it singles out threats to critical infrastructure 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,

[ii] 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.

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.

Absence of critical infrastructure 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 dated 1 March 2014 *On Immediate Measures to Assure National Security, Sovereignty and Territorial Integrity of Ukraine* (enacted by the Presidential Decree No. 189/2014 dated 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 critical infrastructure 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 critical infrastructure 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 critical infrastructure.

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[iii]. 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.

2.2. Sectors, Assets, Systems and Resources Attributable to Critical Infrastructure

Lists of sectors attributed to critical infrastructure 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 critical infrastructure of this country is, probably, the most comprehensive and includes 16 items:

- Chemical;
- Commercial facilities;
- Communications;
- Critical manufacturing;
- Dams;
- Defense industrial base;

[iii] 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 No. 21 (February 2013).

- 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, critical infrastructure is divided into two groups including altogether nine sectors: *vital (absolutely necessary) base technical infrastructure* (energy supply, information and communication technology, transport, water 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 critical infrastructure 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 critical infrastructure sectors is provided in Annex A. The next step following identification of critical infrastructure sectors should be to list individual critical infrastructure 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 critical infrastructure, 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 critical infrastructure 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 critical infrastructure sector.

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

2.3. 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 critical infrastructure, 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[5];
- vitas assets in energy sector[6];
- vitas assets in oil and gas sector[7];
- important governmental facilities, including control centers of government agencies and local government bodies[8];
- potential terrorist targets[9];
- assets to be protected and defended in emergency and during special periods[10];
- assets subject to mandatory protection by State Protection Service on a contractual basis[11];
- high hazard facilities[12] (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[13]);
- assets included in the State Register of Potentially Hazardous Facilities[14];
- radiological hazard facilities subject to development of a facility-level design basis threat (DBT)[15];
- assets assigned civil protection categories[16];
- assets owned by business entities, whose design should account for requirements of engineered civil protection facilities[17];
- emergency service operator - service 112 (free phone number)[18];
- emergency rescue services;
- National Confidential Communication System[19];
- payment systems[20];
- culture heritage sites.

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

3. Main Threats to Critical Infrastructure

Leading nations who declared protection of critical infrastructure 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 critical infrastructure 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 critical infrastructure elements. In this event we speak about the so-called domino effect and/or cascade effect.

As for the spectrum of critical infrastructure 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 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 critical infrastructure. In particular, it should be expected that a high level of terrorist, sabotage and criminal threats to critical infrastructure is likely to persist in a long run as the result of today's crisis.

The existing Ukrainian legal framework governing issues allied to critical infrastructure protection 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 critical infrastructure threats since it has some methodology reservations and blocks some of the advantages offered by implementation of the critical infrastructure protection concept.

It makes more sense to define the following classes of threats for the purposes of critical infrastructure protection:

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 critical infrastructure 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[iv]. According to the State Emergency Service of Ukraine (SESU)[v], 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.

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 critical infrastructure 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.

[iv] *Note:* based on the 2014 National Report on Anthropogenic and Natural Safety in Ukraine (page. 212).

[v] *Note:* based on the 2013 National Report on Anthropogenic and Natural Safety in Ukraine.

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 critical infrastructure.

In addition to the classification by origin, threats to critical infrastructure 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 critical infrastructure protection system. Critical infrastructure protection 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.

4. State Policy in Critical Infrastructure Protection

4.1. The aim of Critical Infrastructure Protection in Ukraine

Enhancement of security and resilience of the national critical infrastructure against the entire range of threats and risks is one of the priority aspects of Ukraine's security policy as it is critical infrastructure 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 critical infrastructure protection in Ukraine is prompted by the critical infrastructure definition and is to secure supply of vital goods and services to the population, society, business and state. For critical infrastructure to perform this function it is necessary to warrant uninterrupted and sustainable operation of critical infrastructure assets in prescribed modes and to be able to prevent destruction or irreparable harm, stoppage or loss of control of critical infrastructure assets as a consequence of effect of all factors, as well as to assure quick recovery of their operation where it was disrupted.

4.2. Strategic Objectives of the State Policy in Critical Infrastructure Protection

Critical infrastructure 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. Critical infrastructure 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 critical

infrastructure. 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[vi];
- 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 critical infrastructure protection policy: *development of security partnership to enhance security and assure resilience of the national critical infrastructure.*

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

Note that in most developed nations main responsibility for security of critical infrastructure 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 critical infrastructure security and conditions for continuing competitiveness of business making required investments in critical infrastructure 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 Germany establishment of trust relationships[vii] 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 critical infrastructure security and conditions for sustaining competitive power of enterprises duly investing in critical infrastructure security should be a mandatory element of such partnership.

Thus the PPP mechanism creates the foundation for promotion of investments in critical infrastructure protection through support of adequate awareness of the business sector of threats and risks for critical infrastructure 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* dated 01 July 2010 No. 2404-VI whose provisions do not apply to critical infrastructure protection activity.

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

[vii] US Department of Homeland Security, National Infrastructure Protection Plan, NIPP 2013. Partnering for Critical Infrastructure Security and Resilience, //www.dhs.gov/national-infrastructure-protection-plan

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 critical infrastructure protection. It also requires development of a legal framework for mutual obligations of the state and non-government subjects in respect of critical infrastructure protection 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 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 critical infrastructure protection should be taken into account both in identification of critical infrastructure assets and in setting requirements for their protection. Any requirements for critical infrastructure protection enhancement, initiated by the state, should be well thought-over considering the above socioeconomic dimension. In addition, for certain critical infrastructure 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 US and elsewhere in the developed world.

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

In the modern world, critical infrastructure elements have sophisticated vertical and horizontal ties, which enables cascade and delayed/remote negative consequences of a failure of a certain critical infrastructure element. As it has been mentioned, in most developed states responsibility for critical infrastructure 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 critical infrastructure 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 critical infrastructure or protected systems becomes important. Where this objective is attained, the partners effectively exchange information (including intelligence) on various aspects of critical infrastructure protection (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 critical infrastructure protection 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 critical infrastructure Ukraine, based on their comprehensive analysis. The following risk management arrangements are expedient for the purpose of risk reduction[viii]:

- enhancement of critical infrastructure resilience to identified threats and hazards;
- prevention of threats related to malicious acts (terrorism, criminal activity, etc.);
- planning timely response to failures in critical infrastructure 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 critical infrastructure functions in case of emergency that cannot be prevented.

Albeit vital importance of critical infrastructure 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 critical infrastructure protection subjects.

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

Ukraine should ensure establishment of the state-level critical infrastructure threats and risks assessment system, proper interface between government 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 critical infrastructure protection 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.

4.3. Main Principles of Critical Infrastructure Protection Policy Formation in Ukraine

Priorities of critical infrastructure protection policy for Ukraine have been formulated based on the significance of critical infrastructure protection 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 critical infrastructure protection 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 critical infrastructure protection tasks;
- consideration of the need for critical infrastructure security in planning, prioritizing and assessment of the nation's socioeconomic development;
- establishment of mechanisms to impact critical infrastructure security state;
- operation of a single center for critical infrastructure security state assessment, threat forecasting and risk assessment for critical infrastructure assets and for coordination of efforts of all stakeholders in critical infrastructure protection;

[viii] US Department of Homeland Security, National Infrastructure Protection Plan, 2006, http://www.naruc.org/publications/nipp_plan4.pdf

- 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 critical infrastructure assets;
- control of all resources available to the state for their rational use;
- implementation of a state-level DBT for critical infrastructure 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 critical infrastructure protection, under which the critical infrastructure protection concept should be implemented through:

- use of a uniform conceptual and methodology framework to analyze critical infrastructure threats;
- development of a methodology to identify (list) critical infrastructure assets based on assessment of importance of goods/services they provide (criticality assessment);
- consideration and assessment of the entire scope of threats for critical infrastructure assets; use of risk-oriented methods for risks and threats analysis and forecast;
- periodical assessment of threats, risks for and vulnerabilities of critical infrastructure assets on the basis of appropriate experience;
- identification of critical infrastructure protection 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 critical infrastructure protection and security.

Public-private partnership principle meaning involvement of all stakeholders in critical infrastructure 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 critical infrastructure protection objectives;
- declaration of asset security by its owner/operator;
- certification of critical infrastructure 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 critical infrastructure assets/systems security;
- involvement of the public and expert community, use of consultative committees to identify requirements for critical infrastructure 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 critical infrastructure operation, international obligations of Ukraine concerning operation and security of critical infrastructure and involvement of Ukraine in European civil protection, cyber security and terrorism suppression mechanisms.

5. Critical Infrastructure Protection System of Ukraine

5.1. Key Tasks of Critical Infrastructure Protection System of Ukraine

Based on the objectives and principles of the critical infrastructure protection system, the following *key tasks* of this system could be formulated.

1) General coordination of critical infrastructure protection in Ukraine, which inter alia includes:

- creation and support of a national center for crisis management and critical infrastructure protection;
- 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 critical infrastructure protection;
- assessment of threats for critical infrastructure 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 critical infrastructure protection 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;
- preparation of a state-level DBT for critical infrastructure;
- 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 (contact card) with EU structures and government authorities of EU member states.

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

- application of existing and establishment of new measured for prevention of potential crises related to operation of critical infrastructure (or individual sectors or assets thereof);
- critical infrastructure 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 critical infrastructure (or individual sectors or assets thereof);
- preparation, within the framework of the national critical infrastructure protection plan, of the plans to prevent crises related to critical infrastructure;

- physical protection of critical infrastructure assets, prevention of unauthorized acts (including acts of terrorism) against critical infrastructure assets, mitigation of negative consequences for and recovery of critical infrastructure assets where unauthorized acts have occurred;
- protection of critical information 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 critical infrastructure assets, development and implementation of engineered security measures for critical infrastructure;
- assurance of stable critical infrastructure 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 critical infrastructure asset data;
- recovery of critical infrastructure operation in the event of an accident/failure, a malicious act that disrupted its operation, or under effects of natural phenomena.

3) *Decision support in critical infrastructure protection,* including:

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

4) *Application of critical infrastructure monitoring and control mechanisms,* including:

- early notification (threat warning) of critical infrastructure asset operators and information, consultative, expert and technological support for critical infrastructure operators and service consumers (the public) for the prevention of, response to and mitigation of potential impact of such threats;
- change of critical infrastructure protection 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 critical infrastructure protection;
- checks and assessment of critical infrastructure asset security;
- checks and assessment of information security at critical infrastructure assets;
- formation, accounting and renewal of critical infrastructure assets certificates and risk cards for localities.

5) *International cooperation in critical infrastructure protection:*

- assessment of transboundary effects of critical infrastructure operation and of transboundary threats;
- exchange of information and best practices in critical infrastructure protection;
- Ukraine's involvement in European mechanisms for critical infrastructure protection;
- analysis of EU 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 critical infrastructure protection system on the above list deserve 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* (the Center). Such institutional novelty should address the task of organizational support for the critical infrastructure protection system. The Center, 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 critical infrastructure protection activities. The functions of the Center should include all those functions that are targeted at addressing critical infrastructure protection 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.

Critical infrastructure protection tasks shift the focus toward prevention of crises related to critical infrastructure 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"[ix] 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."[x] The definition of a crisis situation has a consequential relation to critical infrastructure 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 critical infrastructure (or an individual sector or asset thereof).

Thus it is prevention of crises that should become a key component of the functioning of the *national center for crisis management and critical infrastructure protection*. Potential crises related to critical infrastructure operation should be continuously monitored and identified. This latter task is achievable provided establishment a unit (department) within the Center that will function as a situation center and promptly and on a 24/7 basis address tasks to support decisions in the critical infrastructure protection system. Specifically, such a division within the Center

[ix] From a note to the text of the Law of Ukraine *On Amendment of the Law of Ukraine On the National Security and Defense Council of Ukraine Concerning Improvement of Coordination and Control in the Area of National Security and Defense*

[x] Based on definitions given in sectoral regulations approved by SNRIU orders of 28 August 2008 No. 156 and of 15 September 2011 No. 501/1001.

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 critical infrastructure protection 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 critical infrastructure protection. However, these modes to not correlate with critical infrastructure protection 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[xi], an environmental emergency zone[xii], and law martial[xiii], that are also closely related to critical infrastructure operation protection.

Based on the above and considering the priority of the crisis prevention task for the critical infrastructure protection 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 critical infrastructure 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 critical infrastructure protection 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 critical infrastructure sector, however, due to interface between the sectors (interrelations/interdependence of assets pertaining to different sectors) such a crisis may extend to the entire crisis infrastructure 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 critical infrastructure assets, etc. This mode is applied for critical infrastructure 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.

Identification of principles for economic relationships and their changes in various operation modes should become an important precondition of critical infrastructure 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 critical infrastructure operators amid crisis situations. Lack of clearly formulated responsibilities in case of enhancement of critical infrastructure asset security status should be addressed through adoption of appropriate regulatory documents.

A *national critical infrastructure protection plan* (the Plan) 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

[xi] Law of Ukraine of 16 March 2000 No. 1550-III *On the Legal Regime of Emergency State*
[xii] Law of Ukraine of 13 July 2000 No. 1908-III *On the Environmental Emergency Zone*
[xiii] Law of Ukraine *On the Legal Regime of Law Martial* (revision dated 11 June 2015)

to achieve the system tasks. The Plan should specifically focus on *actions to prevent crisis situations*[xiv] 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 critical infrastructure sectors.

5.2. Subjects of 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 critical infrastructure elements are fully or partly owned by the state.

At the same time, a substantial – and sometimes even prevailing – part of critical infrastructure 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 critical infrastructure resilience remains with owners and operators." In this connection effective public-private partnerships (PPP) in security in general and in critical infrastructure protection in particular are probably the most important component of the government policy in this area.

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

E. g., in the US critical infrastructure security is the responsibility of the Department of Homeland Security established immediately after the 9/11 terrorist attacks. Canada uses a similar approach: like functions are covered by the Ministry of Public Safety and Emergency Preparedness of Canada, except for the issues of maritime safety.

In Germany, activities related to critical infrastructure protection 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 critical infrastructure, analysis of ongoing security environment and development of critical infrastructure protection 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 critical infrastructure protection 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, critical infrastructure is not defined on a legislative level, thus there is no critical infrastructure protection subject. In our state, the Integrated System for Prevention of, Response to and Suppression of Terrorist Acts and Minimization of Consequences Thereof

[xiv] Say, in the UK the government has developed a National Preventive Plan: Gas for gas supply to the energy sector (see) in correlation with general European standards implemented by the Directive No. 2004/67/EU concerning measures to secure uninterrupted natural gas supply.

(Provision approved by the Cabinet Decree No. 1051 of 15 August 2007), the Integrated State Civil Protection System (Provision approved by the Cabinet Decree No. 11 of 9 January 2014), and the State Physical Protection System (Functional Procedure approved by the Cabinet Decree No. 1337 of 21 December 2011) 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 critical infrastructure 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[xv]).

In January 2015, the Ukrainian Cabinet Decree No. 18 approved the Provision on the State Commission for Anthropogenic and Environmental Safety and Emergency Situations (the Provision), as well as the composition of commission members. Pursuant to the Provision, the State Commission for Anthropogenic and Environmental Safety and Emergency Situations (hereinafter the 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.

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 Integrated Gas Transmission System and Interconnected 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 critical infrastructure protection, 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 critical infrastructure protection.

Choice of an organizational model for critical infrastructure protection 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

[xv] *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*

center network having information analysis support for the national situation/crisis center as one of its principal functions.

5.3. Development of Critical Infrastructure Protection Mechanisms for Ukraine

Critical infrastructure protection 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 critical infrastructures and on the assessment of the critical infrastructure protection 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 critical infrastructure protection;
- identification of critical infrastructure priority sectors;
- identification of government authorities responsible for the establishment and implementation of state policy for critical infrastructure protection; clear allocation of responsibilities between all participants of critical infrastructure protection processes/arrangements;
- development and approval of criteria and methods for attribution of assets (irrespective of ownership form) to a critical infrastructure list;
- improvement of a system for critical infrastructure asset condition monitoring, critical infrastructure threat analysis and forecast, identification of methods and ways for critical infrastructure operation related risk mitigation, enhancement of reliability, resilience and sustainability of critical infrastructure assets, prevention of emergencies at such assets;
- improvement of public-private partnership mechanisms, identification of critical infrastructure protection funding sources;
- implementation of innovative developments and improvement of existing means for critical infrastructure assets security and protection;
- development and implementation of standards, regulations and technical conditions for critical infrastructure asset security;
- implementation of a "risk management culture" in operators' management systems;
- improvement of critical infrastructure 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 critical infrastructure protection.

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

a) *For regulatory governance of critical infrastructure protection:*
   - definition of principal terms ("critical infrastructure," "critical infrastructure protection," "critical infrastructure regulator," "critical infrastructure operator," etc.);
   - implementation of a critical infrastructure assets identification procedure (creating a list);
   - implementation of a procedure for the change of a critical infrastructure protection system operation mode depending on the level of threat;
   - governance of information exchange and data acquisition in respect of critical infrastructure 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

situation center for critical infrastructure protection (hereinafter the National Situation Center) and for creation and support of a state-level (national) system (network) of distributed situation 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 National Situation Center as one of its principal functions (see reference information in Annex C);

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

- development of a methodology for qualification of assets as critical infrastructure;
- development of a methodology for identification of condition of critical infrastructure 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 National Situation Center;
- development of recommendations to launch comprehensive target research programs and more intensive involvement of private sector in the funding of critical infrastructure protection research;
- training and retraining of personnel in critical infrastructure protection, 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 critical infrastructure protection issues:

- raising public awareness concerning the main goals of critical infrastructure assets protection, inter alia to deter potential adversaries;
- organization of public-private partnership in security;
- enabling and stimulation of involvement of private sector operators/owners in critical infrastructure protection;
- support of national manufacturers in the security services market (specifically, in cyber security);
- establishment and support of appropriate consultancy, advisory, etc. teams.

6. 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[xvi], followed by its ratification by Ukraine and by some Member States 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 European Union in the field of critical infrastructure protection.

In the European Union, establishment of legal and organizational mechanisms of critical infrastructure protection was initiated in 2004 by the address of European Council to European

[xvi] Association Agreement between Ukraine, on one side, and European Union, European Atomic Energy Community and the member states, on the other side.

Commission, in which European Commission committed to prepare the general strategy of critical infrastructure protection.

In October 2004, the European Commission published official Communication[22] containing review of Commission's activities in this field and propositions regarding additional measures aimed at improvement of European System of Prevention of, Preparedness for and Response to Terrorist Attacks Aimed at EU Critical Infrastructure 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 No. 786 issued in 2006[23], European Commission recommended to all EU countries to take measures stipulated in ECIPP, namely:

- develop national critical infrastructure protection 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 critical infrastructure protection, 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 critical infrastructure facilities;
- identify state authorities responsible for critical infrastructure sectors and corresponding private companies;
- create conditions for efficient interaction and exchange of information, 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 critical infrastructure facilities at the Pan-European level were presented in the Green Paper (2005)[24]. It reviewed 11 critical infrastructure sectors which included 37 subsectors. Then, during preparation of the Draft Directive, 11 sectors out of 29 subsectors[25] were identified, and the approved European Commission Directive[26] now mentions only two European critical infrastructure 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 critical infrastructures in other sectors.

Regarding CIWIN, the main task of this network is generation of tools for coordination and information exchange on critical infrastructure 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 facilities security[27].

So, when developing the critical infrastructure protection 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 European Union's regulations regarding the following:

- general principles of critical infrastructure protection;
- interpretation of basic terms (see Annex D);
- determination of the "Point of contact".
- compliance in terms of critical infrastructure protection's priority (selection of priority sectors and corresponding subsectors of critical infrastructure);

- methodology of comparison and identification of priority facilities in various sectors;
- implementation of current European Union's critical infrastructure protection standards.

It is also worth mentioning that in the course of development of critical infrastructure protection 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 critical infrastructure protection, special attention should be paid to the documents aimed at maximum approximation of the national legislation requirements to the requirements of critical infrastructure 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[xvii]:

- Directive 2005/89/EU of the European Parliament and of the Council Concerning Measures to Safeguard Security of Electricity Supply and Infrastructure Investment;
- Directive 2004/67/EU Concerning Measures to Safeguard Security of Supply of Natural Gas;
- Directive 2005/65/EU of the European Parliament and of the Council of 26 October 2005 on Enhancing Port Security
- Regulation (EC) No. 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[xviii];
- Regulation (EC) No 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[xix].

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.

7. Key Conclusions

The Green Paper covered a wide spectrum of issues related to critical infrastructure protection. This Paper combines analysis of the situation in Ukraine regarding solving tasks of protecting individual groups of critical infrastructure facilities and analysis of experience of critical infrastructure protection 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 critical infrastructure protection system in Ukraine in the future.

a) Today, critical infrastructure protection 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 military and political block. For Ukraine, taking into account complicated security situation, the task of establishment of critical infrastructure

[xvii] See Annex XXVII to the Association Agreement

[xviii] 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)

[xix] Regulation (EC) No 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) No 3051/95

protection 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 critical infrastructure operation. At the same time, implementation of critical infrastructure protection 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. Critical infrastructure protection 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 critical infrastructure protection and, correspondingly, critical infrastructure protection system's tasks and critical infrastructure protection establishment principles. In its turn, system's tasks will drive functions of critical infrastructure protection subjects. Establishment of the state critical infrastructure protection 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 critical infrastructure protection in Ukraine, subjects, tasks and structure of critical infrastructure protection system in Ukraine, to establish responsibilities of the state authorities regarding identification of this system's operation features.

c) The policy of critical infrastructure protection 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 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 operators and the state, both in supporting critical infrastructure protection system operation 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.

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

d) Particular tasks of critical infrastructure protection that differ from the tasks of the existing state civil defense system, counter-terrorism protection, cyber threat counteraction etc. demand organizational novelties, namely, establishment of a Critical Infrastructure Protection Center as a separate body or as a structural part of an authority to be responsible for coordination of actions on critical infrastructure protection. 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 critical infrastructure protection 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.

e) While the Green Paper proposes a list of critical infrastructure sectors along with general structure of criteria of designation of certain facilities as critical infrastructure 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 critical infrastructure facilities without additional analysis.

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

Annex A

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

Table A.1

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, Security Service of Ukraine (SBU)[xxii], Ministry of Internal Affairs[xxiii], State Service of Special Communications and Information Protection of Ukraine (SSC) [xxiv]
2. Transport	Ministry of Infrastructure, SBU[xxi], Ministry of Internal Affairs[xxii]
3. Life Support Networks	Ministry of Regional Development, Construction and Communal Services of Ukraine, State Service of Ukraine for Emergency Situations (SSE)[xxv]
4. Telecommunications and Communication Networks	SSC, Ministry of Internal Affairs[xxii]
5. Financial and banking sector	National Bank of Ukraine, Ministry of Finance, SBU[xxi], SSC[xxiii]
6. Public administration and law-enforcement	SBU[xxi], Ministry of Internal Affairs[xxii], State Guard Service[xxii]
7. Security and defense complex	Ministry of Defense, Ministry of Internal Affairs[xxii], SBU[xxi]
8. Chemical industry	State Service of Ukraine for Labor, SSE[xxiv], SBU[xxi]
9. Emergency services and civil protection	SSE, Ministry of Health
10. Food processing industry and agricultural complex	Ministry of Agrarian Policy and Food

_____

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 counter-action
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
17. National Critical Infrastructure Protection Program
18. National System of Crisis Centers
19. Emergency Response Plans

V. State-Private Partnership in the Field of Critical Infrastructure Protection
20. Tasks and Responsibilities of State Authorities
21. Authority and Tasks of Critical Infrastructure Operators
22. Responsibility of Critical Infrastructure Operators
23. Funding of Measures in the Field of Critical Infrastructure Protection

VI. International Cooperation in the Field of Critical Infrastructure Protection
24. Performance of International Commitments in the Field of Critical Infrastructure Protection
25. Concluding Agreements in the Field of Critical Infrastructure Protection
26. Participation in International Organizations in the Field of Critical Infrastructure Protection

VII. Transitional Provisions
27. Introduction of Modifications to the Laws of Ukraine
28. Development of Regulatory and Legal Acts

Annex C

Additional Information for Section 5

Today, the problem of support of decision making, urgent response to national security threats by fast generation of justified decisions at the highest level of the government control is of vital importance.

The requirement of establishment of a network of emergency response centers, information and analysis centers and crisis centers in the field of national security is becoming more and more obvious. Critical infrastructure protection should be referred to a strategic level of national security measures. In this context, it is reasonable to mention that during the years of independence, there were several attempts to establish a strategic-level crisis center in Ukraine. Thus, the first attempt to create the Crisis Center with the President of Ukraine was made back in 1992. According to the Instruction of the President of Ukraine dated July 14, 1992 No.128/92-rp, the structure of the scientific and technical council on such Center's creation was approved along with the Center's Concept.

Nowadays, there are several centers and systems in Ukraine, which perform or are supposed to perform certain functions of crisis centers in individual national security and defense sectors. Among others, the following agencies should be referred to them:

- *Counter-Terrorist Center with the Security Service of Ukraine* that coordinates activities of counter-terrorist agencies in terms of prevention of, response to and suppression of terrorist acts (including those at extremely hazardous facilities);
- *Crisis Center of Main Command Center of the Armored Forces of Ukraine (MCC of AFU*), whose functions include analysis and generalization of information on emergencies, organization of collection of information on potentially hazardous facilities of the Ministry of Defense of Ukraine;
- *Governmental Emergency Information and Analytical System (GEIAS),* whose establishment program was approved back in 1996, and this program's implementation was approved for the period of 2000-2002. Unfortunately, due to some reasons like inefficiency of the government machine, this system was never implemented in full scope.

The latest attempt in this direction was made in the Administration of National Security and Defense Council of Ukraine (NSDCU) during 2010 through 2013. The Instruction of the NSDCU's Secretary dated November 6, 2013 No. 70 "On Approval of Concept of Establishment of Crisis Center for Information and Analytical Support of the NSDCU Administration" approved the concept and, in the scope of the first phase of works, the soft and hardware complex of this crisis center was created. The need to establish a national crisis center was reflected to certain extent in the Civil Defense Code of Ukraine approved in 2012.

This Code mentions a state emergency control center that performs functions on performance of day-to-day operations control of civil defense subjects, on coordination of control authorities and civil defense forces, on 24-hours-a-day duty and operation of the system of collection, processing, generalization and analysis of information on situation in emergency areas (Article 73, item 1)[28].

Nowadays, individual subsystems of the integrated state civil defense system operate involving institutional structural divisions that perform a part of functions inherent to a crisis center. For example, the SNRIU's structure has operating Information and Emergency Response Center which is a key element of the Nuclear Installations Security Subsystem[29].

Crisis centers are being established and developed in some large corporations, for instance, in nuclear power sector. For example, NNEGC Energoatom is planning to introduce a new RODOS system (Real-time On-line Decision Support System), which is already in operation in some Member States, and to establish a Radiological Accident Consequences Forecast Center, an automatic meteorological station and a specialized computer center.

Availability of a number of sectorial and even corporate crisis centers in Ukraine, a trend of their further development, as well as available foreign experience demonstrate that the task of establishing a national crisis centers network and a national crisis center that should play key roles

in protecting critical infrastructure in Ukraine should be treated as priority category in the field of national security.

Annex D

Basic Definitions in the Field of Critical Infrastructure Protection Used in Regulatory and Legal Acts of the European Union (European Commission Directive 2008/114) and of the USA

Definitions in English published in the official source of the European Commission
'critical infrastructure' means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions
'European critical infrastructure' or 'ECI' means critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure
'risk analysis' means consideration of relevant threat scenarios, in order to assess the vulnerability and the potential impact of disruption or destruction of critical infrastructure
'sensitive critical infrastructure protection related information' means facts about a critical infrastructure, which if disclosed could be used to plan and act with a view to causing disruption or destruction of critical infrastructure installations
'protection' means all activities aimed at ensuring the functionality, continuity and integrity of critical infrastructures in order to deter, mitigate and neutralise a threat, risk or vulnerability
'owners/operators' means those entities responsible for investments in, and/or day-to-day operation of, a particular asset, system or part thereof designated as an European Critical Infrastructure under this Directive 2008/114/EC.

List of References

[1] GREEN PAPER ON A EUROPEAN PROGRAMME FOR CRITICAL INFRASTRUCTURE PROTECTION, http://eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0576en01.pdf

[2] Communication from the Commission of 12 December 2006 on a European Programme for Critical Infrastructure Protection, http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0786en01.pdf

[3] A Communication on Protecting Europe's Critical Energy and Transport Infrastructure (this document contains sensitive information and is not subject to publication)

[4] COUNCIL DIRECTIVE 2008/114/EC of 8 December on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

[5] Decree of the Cabinet of Ministers of Ukraine dated 23.12.2004 No. 1734 "On Approval of List of Enterprises That Are of Strategic Importance for National Economy and Security"

[6] Decree of the Cabinet of Ministers of Ukraine dated 28.07.2003 No. 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"

[7] Instruction of the Cabinet of Ministers of Ukraine dated 27.05.2009 No. 578-p "On Approval of List of Critical Oil and Gas Industrial Facilities"

[8] Decree of the Cabinet of Ministers of Ukraine No. 1051 dated 15.08.2007 (confidential)

[9] Provision on Integrated System for Prevention of, Response to and Suppression of Terrorist Acts and Minimization of Consequences Thereof (approved by the Decree of the Cabinet of Ministers of Ukraine No. 1051 dated 15.08.2007)

[10] Decree of the Cabinet of Ministers of Ukraine dated 24.04.99 No. 675-019 "On Approval of List of Objects to be Guarded and Defended in Emergency and During Special Period"

[11] Decree of the Cabinet of Ministers of Ukraine dated August 10, 1993 No. 615 "On Measures on Improvement of Security for Assets of State and of Other Type of Property" (with modifications)

[12] Law of Ukraine dated 18.01.2001 No. 2245-III "On Extremely Hazardous Facilities"

[13] List of Extremely Hazardous 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 dated 06.05.2000 No.765

[14] Decree of the Cabinet of Ministers of Ukraine dated 29.08.2002 No. 1288 "On Approval of the Provision on the State Register of Potentially Hazardous Facilities"

[15] Order of SNRIU dated 17.12.2012 No. 238 "On Approval of List of Radiological Hazardous Facilities in Ukraine, for Which Facility-Level Design Basis Threat Should Be Developed"

[16] according to the procedure approved by the decree of the Cabinet of Ministers of Ukraine dated 02.03.2010 No. 227 dsk (with modifications as per Decree of the Cabinet of Ministers of Ukraine dated 24.07.2014 No. 545 dsk)

[17] approved by the Decree of the Cabinet of Ministers of Ukraine dated 09.01.2014 No. 6

[18] Law of Ukraine dated 13.03.2012 No.4499-VI "On the System of Public Emergency Care Via Single Telephone Number 112"

[19] Law of Ukraine dated 10.01.2002 No. 2919-III "On the National Confidential Communication System" (with modifications)

[20] Law of Ukraine dated 05.04.2001 No. 2346-III "On Payment Systems and Money Transfer in Ukraine"

[21] Law of Ukraine dated 08.06.2000 No. 1805-III "On Cultural Heritage Conservation"

[22] 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). – [Electronic resource]. – Access mode: http://eur-lex.europa.eu/

[23] Communication from the Commission on a European Programme for Critical Infrastructure Protection
(COM/2006/786 final). – [Electronic resource]. – Access mode: http://eur-lex.europa.eu/

[24] Green Paper on a European Programme for Critical Infrastructure Protection (COM/2005/576 final). –
[Electronic resource]. – Access mode: http://eur-lex.europa.eu/

[25] 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). – [Electronic resource]. – Access mode: http://eur-lex.europa.eu/

[26] Council Directive 2008/114/EC "On the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection". – [Electronic resource]. – Access mode: http://eur-lex.europa.eu/

[27] 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). – [Electronic resource]. – Access mode: http://eur-lex.europa.eu/

[28] Civil Defense Code of Ukraine http://zakon1.rada.gov.ua/laws/show/5403-17/page4

[29] Provision on Functional Subsystem of Integrated State System of Prevention of and Response to Man-Induced and Natural Emergencies, Nuclear Installations Security System http://www.snrc.gov.ua/nuclear/uk/publish/article/140508