Date of publication MAR-30, 2022, date of current version DEC-21, 2021.
www.computingonline.net / computing@computingonline.net

Print ISSN 1727-6209
Online ISSN 2312-5381
DOI 10.47839/ijc.21.1.2515

Prevent and Reduce the Risk of Implementing the Main Cybersecurity Threats

YURIY DANYK, SERHII VDOVENKO, SERHII VOLOSHKO
Ivan Chernyakhovsky National Defense University of Ukraine, Povitroflotsky avenue, 28, Kyiv-049, 03049, Ukraine
(e-mail: zhvinau@ukr.net, vsg64@ukr.net, sergijvolosko@gmail.com)

Corresponding author: Serhii Vdovenko (e-mail: vsg64@ukr.net).

ABSTRACT In hybrid conflicts of any intensity, hostilities (operations) are an element of other (non-force) actions mutually coordinated according to a single plan, mainly economic, political, diplomatic, informational, psychological, cyber, cognitive, etc. This creates destabilizing internal and external processes in the state that is the object of aggression (concern and discontent of the population, migration, acts of civil disobedience, etc.). The article examines the effective organizational and technical countermeasures against hybrid threats, national cyber defense systems in the developed countries. The article also presents the results of the investigations into the effects of the information hybrid threats through cyberspace on social, technical, socio and technical systems. The composition of the system of early efficient detection of the above hybrids is proposed. The results of the structural and parametric synthesis of the system are described. The recommendations related to the system implementation are given. A number of sufficient components for the effective design and development of the national cyber defense system of the state are proposed.

KEYWORDS cognitive warfare; cyber challenges and threats; cyber defense; cyber security; cyber space; hybrid threats; national cyber defense system; system of cyber threats early detection.

I. INTRODUCTION

NOWADAYS combat and other actions (economic, political, energetic, information and cyber) in modern military conflicts known as Hybrid warfare are correlated in idea (concept) and objectives.

Discussions of hybrid warfare have often centered on definitional debates over the precise nature of the term, and whether hybrid covers what other military experts describe as nonlinear warfare, full-spectrum warfare, fourth-generation warfare, or other terms. Similarly, discussions of cyber conflict have treated the phenomenon as a separate domain, as if using cyber tools remained distinct from other forms of conflict. A hybrid war that is de jure being conducted on the territory of Ukraine, and de facto encompassing more participants all over the world, in terms of its content, forms and methods of conducting- can be considered a specific variant of fourth-generation wars (4GW).

Hybrid wars are not declared and, therefore, cannot be completed in the classical sense of the end of wars and military conflicts. This is a kind of permanent war of variable intensity across multiple sectors, with cascading impacts and synergistic destructive manifestations, in which the entire population of the country and the international community are to a certain extent consciously or unconsciously involved. The impacts are felt on all spheres of life, on all sectors of society and throughout the state. Thanks to the use of innovative technologies, it became possible to shift conflict from predominantly overt and forceful (kinetic) means, to less obvious strategies focused on the structural vulnerabilities of adversaries, including (importantly) achieving cognitive advantage over them.

The intensive development of innovative technologies has resulted in new highly technological vulnerabilities in all spheres of life activities of the countries. These effects make it possible to take control and dominate over the basic institutions of the country, as well as to succeed in actualizing their interests through the unconventional and cognitive EFFECTS.

The above cited has resulted in the emergence of a new type of wars in which the main part is assigned to unconventional and mostly asymmetric actions, whereas the military intervention can either be absent or have a reserved character. Such warfare [1, 2] was named “information and cyber warfare (conflicts)”, and the threats realized in these wars were characterized as hybrid ones [3].

Cyberspace proved the main theatre of asymmetric actions [4]. It is promoted by the fact that cyberspace has an extraterritorial, universal and global character; it is also ill-adapted to national geographic borders, can serve as socializing surrounding for people of nearly all ages and is constantly expanding. The nature of cyberspace makes it possible for its users to be mobile and act anonymously, and for the source of message (electronic resource) to be reserved or coded. Communication through cyberspace becomes almost momentary. The information flows can be realized through both the dialogue with mass audience, and the possibility of ultimately individual communication. For the time being cyberspace proves to be the most important instrument of shaping the collective and individual consciousness and the system of values [5]. Along with it the impact itself can be efficient, creative, consolidating and at the same time destructive [6].

The analysis of numerous references makes it possible to ascertain that well-known approaches to detecting hybrid effects and vulnerabilities in cyberspace can be focused on somewhat reduced understanding of their nature [8-14].

In reality one can observe the totality of diversified effects through cyberspace. The above results in the formation of target-oriented effects for realizing the goal of the entire complex of measures aimed at implementing hybrid threats. Along with it, the ultimate goal can be realized only on the basis of complementarity and interaction, as well as on the basis of synergy of all planned measures with respect to their cause and effect relationships.

Thus, it is pointed out [15] that in 60% of cases the measures of cyber operations intersect with the measures of electronic warfare, and in 80% – with the measures of signals intelligence. Cyberspace is used for conducting psychological operation and computer network operations, etc.

Along with it, it is not a force impact on the enemy, but the information, cybernetic and psychological impacts that proves the basic means of realizing the objective. These effects are focused on disabling the enemy, promoting the prearranged narratives, controlling the cognitive sphere on the emotional, moral, cultural and mental levels; forming the system of stable stereotypes and the perception of reality in their context; the critical elements of crisis situations in social, technical, socio and technical systems of different origins prove the result of such effects.

Under the crisis situation (CS) one can understand the totality of conditions and circumstances created by implementing the information, psychological and cyber threats (terroristic, economic, military, diplomatic, ideological, technological, etc.) which are focused on the critical elements on the infrastructure of the state, society, its leadership and security sector, technical and ergatic components of management system (of the state, critical objects, troops and weapons) which bring about the drastic worsening of all indices of the functioning of objects and entities, taken both separately and in totality, up to the complete disturbance (failure) in the activities, including the accompanying profound systems disturbances in the state life activities.

The efficient counteraction to the crisis situations in cyberspace can be obtained by means of the operative detection, defense and active counteraction to the information hazards of a hybrid origin in cyberspace.

That is why of primary importance is the early detection of hybrid effects which create the prerequisites for the emergence of crisis situations on the basis of analysis and prognostication of short-term, middle-term and long-term aftereffects from impacts revealed and effects displayed, which in its turn requires the introduction into practice of substantiated indicators and indices of the destructive activity in cyberspace, the synthesis of methods, models and algorithms of its integrated monitoring and the availability of the corresponding specialized systems.

The shift away from the devastating actions to the ones with mostly functional and structural impact on the adversary has become possible due to the innovative technologies. And the most important thing is reaching cognitive advantage over the adversary. Studies have shown that the cognitive confrontation has become the integral part of contemporary and future wars and armed conflicts both inter- and intrastate ones and between different geopolitical and regional actors. The cognitive element plays an exclusive role among factors that form and cause armed conflict, influence on its course, results, intensity and implications. That is why the contemporary wars and, especially, the wars of the future are fought for the cognitive sphere of the community (society, social groups, people, and population) and for the control over the cognitive sphere. The cognitive impacts can be deliberate and accidental, comprehensive and multi-pronged, of general orientation or targeted. They can be directed at the entire society or on its part, or even on the individuals. They can also be focused on short-term or long-term effects, immediately or after the latent phase, with or without the variation of values, etc. In the contemporary context the conflict participants seek to gain control over the cognitive space, that covers the perception, awareness, beliefs, understanding and values, the intellectual environment of individuals, social groups and society as a whole, where the decision-making process takes place. That is why the main result of the successful cognitive impacts is the change of the model of the world and how it is perceived by the individual, social groups and by the entire society. It gives the possibility to take over and to carry out the external control on the emotional, spiritual, cultural, philosophical and mental levels with the creation of persistent stereotypes that influence the perception of reality. The particular problem in this context is the imposition and promotion of the wrong scientific, state, military theories, paradigms, concepts, strategies that can be effectively implemented and promoted through the scientific and educational institutions. To that end all available opportunities of strategic communications are used, the informational, psychological, cyber and other activities (actions, operations, etc.) are conducted. These activities are directed at the parties to a conflict, the population of participating countries and the world community. The specific feature of such activities is the fact that even if they are conducted by the state actors in a planned and coordinated manner (that is usually not the case) they take place amidst the chaotic deliberate and accidental impacts of all other actors. It transforms into the cyber-informational and cognitive variant of the "war of all against all" (in the cyber and informational space). Eventually, as it is shown in the research, the objects of the cognitive actions are directed at, can be not only induced into the cognitive resonance or dissonance, but also get informationally and cognitively injured, achieve the cognitive borders of perception (inability to perceive the cognitive impacts safely), partial of full cognitive disorientation and even to the cognitive collapse with further transformation into the state of cognitive aggression, depression, disappointment in everything and apathy.

To date the forecast future destructive activity in a cyberspace, that is characterized by diversity and complexity, jointly with asymmetric ness of actions, result in the origin of chain and synergetic destructive effects in different, associate on a cyberspace, spheres influencing on all aspects of everyday life and national security.

Nick Harvey, Minister of the Armed Forces of the United Kingdom (2010-2012), in an interview with The Guardian 31.05.2011 stated: "Cyber weapons now an integral part of Britain's armor". He also said: "Cyber operations will be part of the battles of the future, which will be conducted in parallel with more traditional naval, ground and air space operations. Cyber weapons will become an integral part of the state's arsenal".

To prevent, timely detect destructive cyber impacts, assess risks and effectively counter cyber threats, cybersecurity systems of various levels (or state, departmental, object (especially for critical infrastructure), strategic and tactical in the military sphere) are created in which complex organizational and technical measures are implemented.

At the same time, adequate and prompt response to the challenges and threats associated with innovative developments of software and hardware and methods of cyber-social actions used for destructive actions in cyberspace and through cyberspace are of particular importance.

To do this, cybersecurity systems must have adaptive properties and the ability to transform and reorganize, in accordance with changes in technologies, forms and methods of destructive cyber actions.

This leads to the need for constant development of methodological and technical solutions and tools, forms and methods of combating cyber threats, as well as organizational and technical measures to meet the challenges and threats of the present and future [1-5].

II. ORGANIZATIONAL MEASURES FOR STATE CYBER SECURITY SUPPORT

In the modern conditions a considerable part of conflicts and confrontations between the states and non-state actors are shifting to the cyberspace.

Given the experience of hybrid conflicts and local wars, in which there was confrontation in cyberspace, we can identify the following main forms of cyber action: cyberattacks, cyber actions, cyber operations and cyber campaigns, among which a special place is occupied by cyber operations.

Cyber operations as a specific type of confrontation can be characterized by the following features:

- cyber operations take place in a cyberspace which is real and can be considered as an area of confrontation as any other type of space: cosmic, marine, air and ground;
- most cyber operations are asymmetric (for example, the state with the small army is able to inflict serious losses to the state which has considerably bigger armed forces);
- the consequences of cyber operations in a cyberspace have a direct or mediated effect on all spheres of life in the state and the processes of globalization, which take place in the world (economy, finances, weapon and armament control system, industry, etc.);
- cyber operations affect the cognitive and emotional processes in the society, adequacy of perception and rightness of evaluation of the ongoing events, as well as the quality of decisions made;
- cyber operations do not have the unique generally accepted strategy and are characterized by the large degree of vagueness in relation to tasks, place and time of their lead through;
- it is quite difficult to recognize the targeted or spontaneous cyber operations in real life;
- the conduct of cyber operations in a cyberspace needs creation, implementation and support of the effective system of cyber security. The key elements of such system might be strength and capabilities of cyber intelligence, which according to the areas of responsibility are united under the auspices of a single state interdepartmental coordinating body with the involvement of public, business, educational and scientific component, etc.;

- cyber operations are limited by boundaries of cyberspace and not by geographical borders or time;
- cyber operations unlike other types of military operations are carried out by the opposing parties discreetly and have a high degree of anonymity;
- as a rule, it is difficult to analyze and detect the source of cyber operations;
- cyber operations are based on methodology of integrated application of all existing strength and capabilities, support capabilities or any means related to their use.

Successful achievement of cyber operation goals and qualitative decisions in cybersecurity and cyber defense domain, are directly connected to the fact that their actors are aware of all spectrum of necessary and sufficient conditions for their successful implementation. Consequently, during the cyber operations their goals and tasks, forms and methods of implementation can change and diversify.

Therefore, in order to provide effective cyber security and cyber defense of the state, it is necessary to carry out the following according to a single plan:

- to form and implement the state policy, conceptions, strategies, programs on information security, cyber security and cyber defense; to form and implement the policy of the Ministry of Defense and the Armed Forces in a cyberspace;
- to implement the measures on creation and development of information and cyber systems and resources in the Armed Forces;
- to coordinate the actions of information and cyber security actors; to develop the standards of specialists training on information security, cyber security and cyber defense; to organize the co-operation and implementation of measures (including the preparation of the state to the cyber defense) with structural subdivisions of other central executive institutions and international partners on matters of cyber security and cyber defense;
- to organize and maintain cooperation with the computer emergency response team and computer security incident response team (CERT/CSIRT); to plan and coordinate the management of actors activity in a cyberspace according to a single plan and to control their actions; to monitor and analyze the cyber incidents, destructive informative and cognitive actions in a cyberspace; to detect the vulnerabilities of friendly and enemy cyber systems through the cyberspace and effectiveness of the cyber defense;
- to plan, organize and coordinate the intelligence (Cyber Warfare Intelligence), defensive (Defensive Cyber Warfare) and offensive (Offensive Cyber Warfare) operations in a cyberspace (Cyberspace Operation) and cyber operations (Cyber Operation); to organize and co-ordinate the cybernetic, electronic, network, informative, cognitive and psychological operations in a cyberspace (including social networks).

It should be also mentioned that the profile structure can unite all existing units that are involved in resolving the issues of the cyber defense in a single system for their effective actions under a unified leadership and, with a single design and plan. The absence of profile structure constrains the national system formation for ensuring cyber security in the defense sector.

Global experience shows for the troops the only way to fulfill the tasks effectively and to make full use of armaments is bringing them together into a single structure (according to the area they operate or to the armaments and equipment they use) with the rational command and control system from the strategic to the tactical levels. As an example – the development of aviation and the wide-spread proliferation of tanks and air-defence systems in the beginning of the 21st century raised an issue of establishing appropriate institutions and their governing bodies. It is known that before these systems rational command and control systems were created the effectiveness of forces and resources application had been extremely low.

According to this principle the Cyber Command that was finally formed in 2009, included the structures that are responsible for: operations in the computers, networks, electromagnetic spectrum of radiation, information and psychological operations, organization of the technological types of intelligence, provide the communication and the cryptology protection of the information, take part in the deception operations.

The basic trend of its creation was the integration of different directions of activity that are related to the cyberspace (and the relevant subdivisions) into the single structure. This structure is in charge of the cyber defense according to the goal, tasks, appropriate forms and methods of security in the military sphere.

Thus, in the USA in the “National Defense Authorization Act” for 2018 for the US Ministry of Defense the task is set to centralize the command and control system of all the forces and capabilities, that are related to the cyber defense, active measures in the cyberspace and other operations in the computers’ network, electromagnetic spectrum of radiation, information and psychological operations, the technological types of intelligence, etc. Following this typical structure the Cyber and Information Space Command was established in 2016 in Germany. New Command has the status of the separate armed force that includes the joint units and subdivisions of SIGINT, EW, information and psychological operations, information and technical support (communication), etc. Nowadays the cyber commands are similarly established in many countries of the world as well as the NATO cyber command. In Ukraine this issue is being addressed now. According to the existing legislation the preparation of the country to repel aggression in cyberspace (cyber defense) is one of the main tasks that are set forth for the Ministry of Defense and the Armed Forces of Ukraine. Different structural subdivisions on the different levels of command are responsible for the fulfillment of the cyber defense tasks that are combined by their content and area.

After the adoption of the Law of Ukraine on the main principles of the cyber security in Ukraine in October 2017 the new task was set forth for the Ministry of Defense and the General Staff of Ukraine as to the measures to provide the cyber defense of critical information infrastructure in a state of emergency and in the case of martial law.

The above-mentioned requires the creation of the cyber defense system that will provide the coordinated management of all its components. This system needs the appropriate governing body that from the point of view of the structure, tasks and functions is similar to the corresponding governing bodies of NATO member-countries. This body is intended for the realization of the unified policy and the strategy of actions of the Defense Ministry and the Armed Forces of Ukraine in information and cyber space; organization and coordination of measures as for the cyber space and the protection of state's critical information infrastructure; control of the cyber defense forces under the crisis situations, the specific period and in the case of martial law.

This body that deals with the information and cyber defense security should solve the following tasks:

- participation in the formational and implementation of the state policy in the cyber defense sphere;
- the formation and the implementation of the policy of the Ministry of Defense and Armed Forces of Ukraine as for the actions in the cyberspace;
- the participation in taking measures as for the creation and development of the information systems and resources in the Armed Forces of Ukraine;
- the coordination of actions of the cyber security subjects of the Ministry of Defense and the Armed Forces of Ukraine;
- participation in the development of the training standards and the cyber security specialists preparation that are contracted by the state;
- the organization of cooperation and conducting the activities (including as for the preparation of the country to the cyber defense) with the structural subdivisions of other central bodies of executive power and with international partners on the cyber defense issues;
- the support of the interaction with computer's incidents response teams (CERT/CSIRT) of other governing bodies;
- planning and arranged management of subjects activity in the cyber space based on single idea and plan. The control and coordination of their actions;
- monitoring and analyses of the cyber incidents and the effectiveness of cyber security system activity, finding out the vulnerabilities in own and adversary's cyber systems.

To that end the following departments in the information and cyber security governing body should exist: the cyberspace monitoring; the cyberspace protection; active measures in the cyberspace and cyber operations.

The set of organizational measures to ensure cybersecurity at the state level should take into account the improvement and development of legislation, standardization and certification, educational, scientific and industrial activities, public-private partnerships in information and cybersecurity, as well as their comprehensive and rational resource provision.

It is necessary to determine the set of critical infrastructure facilities, cyber threats to these facilities and the risks of their implementation, as well as to take measures to improve the forms, methods and techniques of their timely detection, prevention, counteraction and neutralization.

The main issues are the training of specialists and scientific support, without which all other issues cannot be solved rationally.

Analysis of the training of cybersecurity specialists for the state economy and the security and defense sector of Ukraine showed problems in the organization and implementation of training and its quality, as well as the lack of a common methodology, standardization and unification of basic aspects of training.

The reason for the low quality of education on cybersecurity is often insufficient capacity (financial, technical, methodological, personnel, etc.) of educational institutions to train specialists in this specialty and conduct research, duplication of structures with related areas and objectives, irrational waste of financial, logistical and human resources.

In the security and defense sector, the issue of concentration of specialists, resources, and all efforts in a single dedicated specialized educational and scientific institution in high-tech defense areas, which are united by their attitude to cyberspace, information, cybersecurity and cyber defense is also unresolved. As a result, organizations face the problem of insufficient staffing, in the absence of a systematic approach to training for this area.

It is established that in order to increase the efficiency and quality of training of cybersecurity specialists there is a need to develop and improve the existing training system, guidelines, methodological support for training, elimination of differences in views on goals, objectives and content of training in general. Moreover, the provision of standardization and the creation of a rational system of education, scientific and scientific and technical activities in this area will ensure the proper quality of research and training of cybersecurity professionals.

III. TECHNICAL MEASURES FOR STATE CYBER SECURITY SUPPORT

Technical measures to ensure cybersecurity at the state level, as research has shown, should include addressing the issues of timely provision of all government agencies and structures with modern hardware and licensed software products, the availability of comprehensive information security systems, hardware and software to detect malware, fix and identification of cyber incidents.

Existing cyber polygons should be integrated into a single system, with the possibility of their use, both for research and training with the integration of modeling bases. Establishment of a system of constant automatic control of the national segment of cyberspace, both its technical and socio-technical components, development and implementation of new approaches and tools for finding and identifying vulnerabilities in information and cyber infrastructure with continuous software improvement and implementation, for this purpose, machine learning and artificial intelligence products.

At the same time, technical means must provide permanent collection, processing, generalization, systematization and analysis of information about destructive activity in cyberspace, sources of threats, forecasting the situation, protection of social Internet services (video services, GeoServices, etc.).

A special danger, as studies have shown, is the occurrence of chain effects during cyberattacks on various objects and resources.

Destructive impacts are usually accompanied by chain effects and synergetic consequences in all spheres of everyday life. It provokes systematic destabilization of all spheres of everyday life of the population and the state as whole, which are the object for aggression.

After the attack on the Ukrainian power grid, American officials from the Department of Energy, the Department of Homeland Security, the FBI, and the North American Electric Reliability Corporation stepped up their activities, recognizing the need to use this situation to understand the tactics and practice of the aggressors, forecasting the types of future cyber attacks, and developing effective protection measures against them [14]. Collaboration with Ukraine on countering these threats is also considered a critical element of the United States cyber defense.

In modern conditions, the cyber impact on objects of influence is usually accompanied by chain effects that propagate a destructive wave on interacting objects and systems. It is often carried out using strategies and technologies of dispersed-focused actions.

The issue of identifying and resisting the complex dispersed-focused information-cyber impacts with chain effects on various spheres of activity of the state and society at this time is vital and crucial for ensuring the national security of any state.

The chain effect can be explained by the appearance of great number of negative consequences as a result of cyber impact on other spheres and objects related to the target object of the cyber attack. It gives birth to second waves of destructive effects, which provoke even more systematic destructive consequences of the cyber impact.

Analysis of cyber attacks on Ukraine showed the main components of every cyber attack: goal, content, organization, strategy, tactics of realization, main and chain effects, its results and consequences.

Cybercrime actions can be carried out sequentially, simultaneously and sequentially, in parallel, using methods of organization of dispersed-focused actions. Dispersed-focused actions involve cyber impacts on the most vulnerable elements (objects) of the infrastructure. A set of simultaneous and (or) sequential cyber impacts provides synergetic effect on unpredictable places (elements, systems, spheres), which may not be closely related to target object of cyber attack, but will be influenced due to dispersed cyber impact. This method works on design of hybrid cyber attacks with chain effects. It disperses a destructive wave on interrelated objects and systems, having a negative cyber impact on several spheres at once. Cyber impacts can be implemented synchronously/ asynchronously, complex, simultaneously or sequentially. But at the same time, the damage to the objects of influence is systematically destructive and most effective, according to the criterion “efficiency-time-cost”. A combination of research and combat analyses indicates that cyber-related actions and information warfare are increasing in both scope and importance for war fighters. In this context, hybrid warfare and its use of cyber assets is one of the most important factors for understanding the future arc of conflict. Combat actions in Ilovaysk and Debalcevo in Ukraine were preceded by a significant burst of activity in information space. Negative information on key authorities of Armed Forces of Ukraine and government representatives was spread widely (usually outbursts of negative information in the Internet preceded the start of new combat campaign) [17]. A common tactic identified by Duggan as cyber aggression, coupled with disinformation from proxies and false fronts on the internet [21].

Information and psychological operations (actions) of the enemy in cyber space require the use of different Internet resources. The content analysis and modeling in Infostream system concerning actions in Debalcevo in February 2015 illustrate the amplitude fluctuations of quantity critical to the spread messages [17].

Media analysis has demonstrated the significant consequences that can result from the mass usage of widespread, negative social political information campaigns. First, cyber aggression against key figures in government is expected to encourage the widening range of negative information streams in order to aggravate existing civil mistrust and anti-government behavior. When it is extended into social media, the spread of false and malicious information encourages behavior and beliefs that would normally be kept in check by existing social mores and civic expectations. Even if information does not create a conscious change in beliefs, it can impact the interpretation of future information by providing effective anchoring and priming media [18]. This can aid a domestic aggressor wishing to influence the course of the conflict in order to weaken support for the target government. In some cases, such information warfare can take the place of kinetic operations, undermining defensive campaigns before they even need to begin.

Cyber aggression often conceals its actors and motives, shrouded by technological methods that can mask their manipulative goals. The methods of concealment include anonymous claims to authority, news items manipulated with half-truths, repetition of messages, information overload, cyber-pseudo operations (government posing as insurgents), sock-puppeting (government agents playing the role of online commentators), and astro-turfing (creating of false grassroots movements).

The use of cyber assets has been a form of force projection that helps initiate crises far ahead of and beyond the front lines, creating forms of more complex crises that affect energy infrastructure, banking systems, and political leadership, not solely armed forces fighting on the front lines. Again, the extension of traditional military conflict is not a new strategy, but new technologies have been able to provide both the means and vulnerabilities to allow such operations at a scale not often witnessed before, and with a smaller investment in resources on the part of the aggressor.

Studies and research have shown that with the current and ever-increasing intensity of cognitive effects on society in cyberspace and through cyberspace, it is necessary to ensure their timely detection and rapid response to them.

It is expedient to solve this task comprehensively at the international, state, regional and local levels by creating a coordinated functioning, with the exchange of necessary information, a network of centers for counteracting information and cyberattacks.

The software and hardware of such centers, united in a single network, should provide monitoring and detection of destructive effects, analysis of their features, features and mechanisms of implementation. They should identify the sources and options for the distribution of dangerous content, the relationship during the operation (action) between the various Internet resources to determine the purpose of action and possible outcomes.

According to the results of research and practical experience, active information counteraction to destructive information influences is achieved through:

- timely detection of dangerous information and misinformation of their primary sources and causes of spread, assessment of their tone and content, analysis of the nature, content, direction, mechanisms and means of information and psychological operations;
- study, accumulation, systematization and analysis of information on the mechanisms and means of information and psychological actions and operations;
- placing on corresponding to the required target audience resources and in the places of their interests of reliable content on the set informative occasion;
- advising of proprietors of resources about impermissibility of distribution of unverified and unconfirmed information;
- blocking sources of dangerous information and misinformation.

IV. THE SYNTHESIS OF THE SYSTEM OF EARLY DETECTION OF INFORMATION HYBRID EFFECTS IN CYBERSPACE

The report highlights the results of the investigations into (of) the following problems:

- what (which) resources of electronic mass media, blogosphere, social networks must be employed for revealing the information effects through cyberspace;
- what information flows can promote hybrid threats and result in the crisis situation;
- the possibility of detecting real threat;
- necessary means and algorithms of revealing the effects;
- necessary functional elements for creating the integral system of detecting hybrid effects;
- what formations are able to implement the system of early detection of information hybrid effects.

The report shows that the hybrid effects can be described by a set of qualitative a and quantitative r indices: $G_i = \{A_{ji}, R_{fi}\}$, where $i = \overline{1,I}$, $j = \overline{1,J}$, $f = \overline{1,F}$. The indices and indicators are used for simulation and further identification of hybrid threat.

The essential ability of detecting threats within the admissible time, the complexity of identification algorithms is determined by the level of the threat reserved character.

The reserved character of the hybrid effects can be evaluated through the probability of detecting its indications.

$$P_d = \prod_{j=1}^{N}\left(1-\prod_{q=1}^{K}\left(1-P_{d_q}\right)\right), \tag{1}$$

where $P_{d_q} = \dfrac{m_d}{N \cdot l}$ – the predictability of determining the q-stage of the effects realization (m_d – the quantity of cases of q-stage detection, l – the quantity of interactions of q-stage of cyber threat in every N attempt of its realization); K – the quantity of the realization stages.

Resource is the information source (IS) which is described by a set of pairs (data card):

I_{ks}^{ID} – the information abilities of the resource;

TX – the resource technical characteristics: $ID_i = \{I_{ks\ i}^{ID}, TX_i\}$, where $i = \overline{1,Q}$.

The system of early detection of hybrid threats and effects on the basis of analyzing the information activity in cyber space proves most effective when including the following subsystems:

- the analysis of cyberspace and its components;
- the analysis and support of current databases of cyber incidents and threats;
- the activities and research of domain activities in cyberspace;
- the analysis of activities in the blogosphere, social networks and electronic mass media;
- the detection and analysis of technologies of cyber effect on control systems, network (physical and logical) topology, hardware and software services and data center support services (the information center);

- the detection and analysis of the technologies of the information effects on data center (information center) operators by means of cyberspace;
- detection and analysis of the technologies of the information and cyber effects on the critical elements of the infrastructure, subjects and objects of defense and security sector authorities of the state, society and personality under the conditions of hybrid conflicts of various intensity;
- the content analysis. Detection of content, which itself or in combination with other influences leads to the formation of destructive narratives and cognitive dissonance;
- the modeling of measures and means of cyber defense of wire and wireless networks of the data center (information center);
- the modeling of measures and means of cyber defense of the system of control, network (physical and logical) topology, software and hardware services and data center (information center) support services;
- the technologies of the information security of the data center (information center) operators through cyberspace;
- the technology of cryptoanalysis and cryptographic security modeling;
- the modeling of measures, means and technologies of protection from the information and cyber effects of critical elements of the components of the infrastructure, subject and objects of the defense and security sector authorities of the state, society and personality under the conditions of hybrid conflicts of various intensity;
- the modeling and simulation of actions in cyberspace, organization of exercises (training) in cyber security and cyber defense;
- the modeling of cyber-attacks on the cryptosystems of the data center (information center);
- the modeling of socio-technical cyber-attacks through cyber defense on the data-center (information center) operators, subjects and objects of defense and security sector authorities of the state, society and personality under the conditions of hybrid conflicts of various intensity;
- the testing of data center services for cyber security.

Functional blocks and their interrelations are shown in Fig. 1.

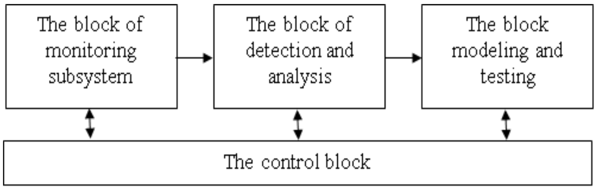
The block of monitoring subsystem
The block of detection and analysis
The block modeling and testing
The control block

Figure 1. Functional blocks of the system.

According to the outline formed the efficiency of the system determines the totality of particle criteria of its subsystems. In the traditional case the system which is being synthesized must meet the following requirements: ensuring the minimum time t_s which is determined for eliminating CS; possessing a high authenticity level of solutions D_s which are formulated for eliminating CS; providing for the best information excessiveness IN_s for taking solutions aimed at eliminating CS. Thus, the list of criteria requirements for implementing the structural synthesis of the system of early detection of information hybrid effects can be presented as follows:

$$\begin{cases} t_s \to \min, t_s \le t_{spor}, \\ D_s \to \max, D_s \ge D_{spor}, \\ IN_s \to \max, IN_{s\min} \le IN_s \le IN_{s\max}. \end{cases} \quad (2)$$

The criteria requirements prove contradictory. Ensuring the highest level of authenticity requires the increase in the number of monitoring sources. This in its turn provides for the increase in time spent on implementing the process of monitoring and information analysis.

The subsystems cited above are realized on the basis of automated working places (AWP) as a universal functional unit.

The efficient measures aimed at detecting hybrid activities, localizing and eliminating specific situations with the use of the cluster-oriented approach require the situational structural and parametric synthesis of the integrated distributed information system of control and situation control of its structure and parameters. The above provides for temporal, structural and functional distribution of tasks related to the processing and analysis of intensive and dense information flows under considerable content dynamics for detecting destructive elements and effects which can result in the emergence of critical situations of various origins.

The technique of the structural and parametric synthesis covers the following stages:

1) Forming the segment of initial data (CS, AWP, IS data cards) in accordance with the information of data base and knowledge base formed a priori.

2) Determining the optimal quantitative composition of AWP subsystems and appropriate IS with the use of optimization models [19].

3) Synthesizing the structure of the system of detecting the information hybrid effects in accordance with [20].

4) Assessing the efficiency of the results of AWP subsystems configuration/

5) In case of changes observed in the current situation *the repetition of points 1-4* is implemented.

The efficient detection and prevention of destructive information and psychological activities of the enemy in cyberspace with the aim of counteracting them operationally stipulate the necessity of creating situational centers whose composition, structure and construction architecture have to include standard and variable sets of specialized AWP with the above cited functions which can be united on the national and international levels in specialized network formations which are created with respect to cluster aggregation principle. They must provide for monitoring and detecting destructive activities and their indicators, mechanisms (strategies, tactics, techniques, forms and methods) of realization.

The measures aimed at neutralizing the destructive information and cyber effects and their sources through cyberspace on the cognitive space can be as follows:

- giving advance notice to web-site owners (if known) about the impossibility of spreading fake or unauthentic, unchecked information, thus recommending them to delete it in case of its hazardous effects on the subjects and objects of national security (personality, society, state);
- blocking web-resources and deleting the content on condition that the web-site owner or moderator cannot be identified and the content itself really poses threat to the subject of object of national security [21].

To ensure the functioning of the system elements which are coordinated in space and synchronized in time the process of the situational structural and parametric synthesis of complex distributive system and the situational control over its structure (Fig. 2) and parameters must be implemented.

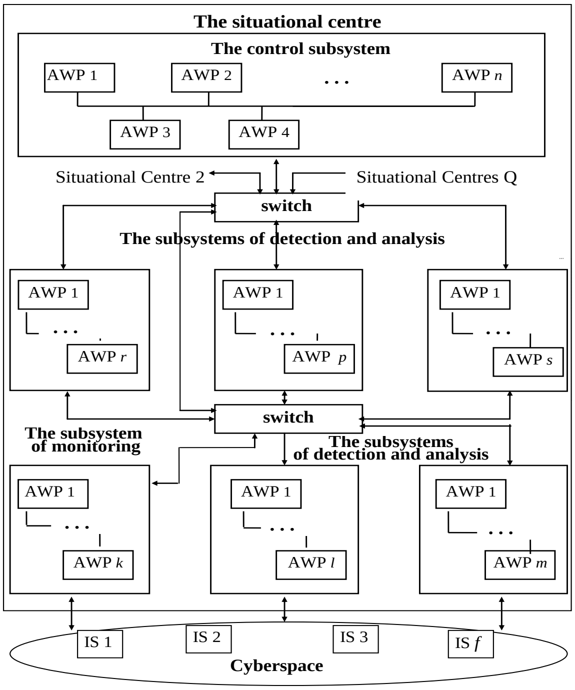

Fig. 2. The structure of situational centre.

V. CONCLUSIONS

Ensuring national security and defense in modern conditions and in the future requires an effective national cybersecurity system.

The basis for the formation of a national cybersecurity system is a comprehensive and systematic approach to the availability and effective implementation of all necessary organizational and technical measures to ensure cybersecurity.

The report considers the crisis situations which emerge as a result of the information and cyber activities of a hybrid character. It also highlights the indices and indicators of the information hybrid effects through cyberspace.

On the basis of analyzing the information activity in cyberspace the author proposes a theoretically substantiated and experimentally proved composition related to the system of early detection of the information hybrid effects.

It is shown that the localization and elimination of a specific critical situation require the situational structural and parametric synthesis of the complex distributive information system of management and situational control. The situational center proves to be its basic element.

The report also dwells on the functions, standard and variable sets of software and hardware complexes of specialized automated working places.

The practical application of software and hardware complexes for the automated realization of the process of monitoring, the analysis of activity in cyberspace prove the possibility of ensuring early detection of information hybrid threats and effects.

References

[1] F. Hoffman, "Hybrid Warfare and Challenges," Joint Forces Quarterly, issue 52, pp. 34-39, 2009.

[2] H. Gunneriusson, "Hybrid warfare: Development, historical context, challenges and interpretations," Icono 14, vol. 19, issue 1, pp. 15-37, 2021. DOI: ri14.v19i1.160

[3] B. Boyer, "Countering hybrid threats in cyberspace," *Cyber Defense Review*, vol. 2, ed. 3, 2015.

[4] N. Iancu, A. Fortuna, C. Barna, *Countering Hybrid Threats: Lessons Learned from Ukraine*, IOS Press BV, Amsterdam, 2016, 286 p.

[5] S. Harris, Cyberwar @: The Fifth Theater of War, 2014.

[6] J. Suler, "The online disinhibition effect," *Cyber Psychology and Behavior*, vol. 7, issue 3, 321-326, 2004.

[7] Cyber War: The Next Threat to National Security and What to Do About It by Richard A. Clarke – http://indianstrategicknowledgeonline.com/web/Cyber_War_-_The_Nex_Threat_to_National_Security_and_What_to_Do_About_It_(Richard_A_Clarke)_(2010).pdf, 2010.

[8] P. Eronen, *Russian Hybrid Warfare: How to Confront a New Challenge to the West*, FDD PRESS, 2016, 27 p.

[9] B. Renz and H. Smith, *Russia and Hybrid Warfare – Going Beyond the Label*. [Online]. Available at: http://www.helsinki.fi/aleksanteri/english/publications/presentations/papers/ap_1_2016.pdf.

[10] Cyberspace Threats and Vulnerabilities. [Online]. Available at: http://www.informationclearinghouse.info/pdf/cyber_warfare_case_for_action.pdf.

[11] P. Cornish, R. Hughes, and D. Livingstone, *Cybers Pace and the National Security of the United Kingdom. Threats and Responses*, A Chatham House Report, March 2009.

[12] What is Cyber Threat Intelligence, and why you Need It, 2017 [Online]. Available at: https://blog.unloq.io/what-is-cyber-threat-intelligence-and-why-you-need-it-fd33e24954da.

[13] M. Mateski, C. Trevino, and C. Veitch, et al. Cyber Threat Metrics. Sandia National Laboratories Report, March 2012.

[14] J. Andress, S. Winterfeld, R. Rogers, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, Amsterdam: Syngress/Elsevier, 2011, 289 p.

[15] I. R. Porche III, C. Paul, M. York, et al., *Redefining Information Warfare Boundaries for an Army in a Wireless World*. [Online]. Available at: https://www.rand.org/content/dam/rand/pubs/monographs/mg1100/mg1113/rand_mg1113.pdf.

[16] Putin's asymmetric assault on democracy in Russia and Europe: implications for U.S. National security a minority staff report prepared for the use of the committee on foreign relations United States Senate one hundred fifteenth congress second session January 10, 2018. [Online]. Available at: http://www.gpoaccess.gov/congress/index.html

[17] Information operation against Ukraine Armed Forces officials "If not the Generals…," http://colonelcassad.livejournal.com/2474409.html, http://www.segodnia.ru/content/168270, https://topwar.ru/85589-esli-by-ne-generaly-pozornaya-istoriya-ukrainskoy-armii.html

[18] Yu. Danyk, O. Pisarchuk, "Method of structural parametric synthesis of complex ergatic distributed informational-controlling system of response on conflict situation," *Journal of Automation and Information Sciences*, Begell Hours, inc publishers, USA, vol. 46, issue 3, pp. 47–69, 2014.

[19] Yu. Danyk, T. Maliarchuk, Ch. Briggs, "Hybrid war: High-tech, information and cyber conflicts, connections," *The Quarterly Journal*, vol. 16, no. 2, pp. 524, 2017. URL: http://www.jstor.org/stable/26326478.

[20] E. Stoycheff, E. C. Nisbet, "Priming the costs of conflict? Russian public opinion about the 2014 Crimean conflict," *International Journal of Public Opinion Research*, vol. 29, issue 4, edw020, 2016.

[21] P. Duggan, "Strategic development of special warfare in cyberspace," *Joint Force Quarterly*, vol. 79, pp. 46-53, 2015.

YURIY DANYK, Doctor of Sciences (Engineering), Full Professor, Major general. Science interest: Information and Cyber security, and Cyber Defense. https://orcid.org/0000-0001-6990-8656. E-mail: zhvinau@ukr.net.

SERHII VDOVENKO, Master of State Military Management in the field of defense, Associate Professor of Communications and Automated Control Systems Department of National Defense University of Ukraine named after Ivan Chernyakhovsky, Colonel. Science interest: Cryptography, Information and Cybersecurity and Cyber Defense. https://orcid.org/0000-0001-8139-7975. E-mail: vsg64@ukr.net.

SERHII VOLOSHKO, Candidate of Technical Sciences, Senior Researcher, Chief Specialist of the Military-Scientific Department of the General Staff of the Armed Forces of Ukraine, Colonel. Science interest: Digital Signal Processing. http://orcid.org/0000-0001-8953-4663. E-mail: sergijvolosko@gmail.com.