Ministry of Education and Science of Ukraine
Poltava State Agrarian Academy

SECURITY MANAGEMENT OF THE XXI CENTURY: NATIONAL AND GEOPOLITICAL ASPECTS. ISSUE 2

Collective monograph

In edition I. Markina, Doctor of Economic Sciences, Professor

Nemoros s.r.o.
Prague, 2020

Recommended for publication by Academic Council of
Poltava State Agrarian Academy
(Protocol No. 13 dated 5 February 2020)

Recommended for publication by Academic Council of
the Institute of education content modernization of
the Ministry of Education and Science of Ukraine
(Protocol No. 1 dated January 29, 2020)

Recommended for publication by Scientific Institution of
the Information Systems Management University
(Protocol No. 1-20 dated February 04, 2020)

The monograph is prepared in the framework of research topics: «Management of national security in the context of globalization challenges: macro, micro, regional and sectoral levels» (state registration number 0118U005209, Poltava State Agrarian Academy, Ukraine), «Macroeconomic planning and management of the higher education system of Ukraine: philosophy and methodology» (state registration number 0117U002531, Institute of education content modernization of the Ministry of Education and Science of Ukraine, Ukraine), «Infocommunication aspects of economic security» (Protocol 1-20 of February 04, 2020, Information Systems Management University, Latvia).

ISBN 978-611-01-1814-9

Nemoros s.r.o.,
Rubna 716/24, 110 00, Prague 1
Czech Republic, 2020

PREFACE

The issues of security management in the conditions of the modern environment instability are of top-priority and stipulate continuous scientific research on the topics of the global and national economic, technological, food, energy security, innovation aspects of forming social, educational, and information security, management of economic security in conditions of integration processes and other.

In the early 21st century, the world faces with cardinal transformations accompanied by changes in geopolitical configurations, integration processes and other changes that affect the state of national and geopolitical security. The events of the last decade have revealed an exacerbation of the problems of global security and the ambiguous impact of the processes of globalization on the development of different countries. Under the circumstances, the rivalry between the leading countries for redistribution of spheres of influence is stirring up and the threat of the use of force methods in sorting out differences between them is increasing. The global escalation of terrorism has become real, the flow of illegal migration and the probability of the emergence of new nuclear states are steadily increasing, and international organized crime is becoming a threat. In addition, in many countries there is an exacerbation of socio-political and socio-economic problems that are transforming into armed conflicts, the escalation of which is a real threat to international peace and stability. These and other factors have led to the fact that the potential of threats to global and national security has reached a level where, without developing a system state policy to protect national interests and appropriate mechanisms of its implementation, there may be a question of the existence of individual countries as sovereign states.

The threat of danger is an immanent, integral component of the process of civilization advancement, which has its stages, parameters and specific nature. Obviously, the problem of security in general, and national one in particular, should be objectively considered in terms of its role participation in the development process, that is, to set it up as both destructive and constructive functions (as regards the latter, it is necessary to emphasize the undeniable fact that the phenomenon of safety is based on counteraction to the phenomena of danger, the necessity of protection from which exactly stimulates the process of accelerating the search for effective mechanisms of counteraction).

The formation of new integration economic relations in Ukraine and the intensification of competition objectively force managers of all levels to change radically the spectrum of views on the processes of formation and implementation of the security management system in unstable external environment that is hard to predict. Today, the main task is to adapt not to changes in market conditions of operation, but to the speed of these changes. In this regard, there is a need to develop effective security management mechanisms that are capable of responding adequately and in due time to changes both in the internal and external environment.

Therefore, this problem is being paid more attention in theoretical research works of scientists and practical activity of business entities.

Taking into account the fact that the traditional means of national and geopolitical security as a mechanism in its various models, forms, systems have reached their limits, since they do not contribute to solving the problems of globalization of the civilization development, there is an objective need to form a paradigm of security management in the 21st century, which aims to confront destruction processes; to harmonize activities of socio-economic systems: society, organization, the state, the world. The joint monograph «Security management of the XXI century: national and geopolitical aspects. Issue 2» is devoted to these and other problems. The progress in the development of the theory of security management on the basis of the analysis of theoretical and methodological works of scientists and the experience of skilled workers presented in the joint monograph creates opportunities for the practical use of the accumulated experience, and their implementation should become the basis for choosing the focus for further research aimed at improving the security management system at the national and international levels. In the joint monograph, considerable attention is paid to solving practical problems connected with the formation of the organizational and legal mechanism of organization of the security system in terms of globalization by developing methods, principles, levers and tools of management taking into account modern scientific approaches.

In the monograph, the research results and scientific viewpoints of the authors of different countries are presented in connection with the following aspects of security management: national security, food, environmental and biological security, economic and financial security, social security, personnel and education security, technological and energy security, information and cyber security, geopolitical security.

The authors have performed a very wide range of tasks – from the formation of conceptual principles of security management at the micro, macro and world levels to the applied aspects of management of individual components of national security.

The monograph «Security management of the XXI century: national and geopolitical aspects. Issue 2» consists of four parts, each of which is a logical consideration of the common problem.

The structure of the monograph, namely the presence of particular parts, helps to focus on the conceptual issues of the formation and development of national, economic, financial, social, food, environmental, biological, personnel, educational, technological, energy, information, geopolitical security, and problems of the maintenance of the practical process of application of the developed cases.

The joint monograph is prepared in the context of three research topics: «Management of national security in the context of globalization challenges: macro, micro, regional and sectoral levels» (State registration number 0118U005209); «Macroeconomic planning and management of the higher education system of Ukraine: philosophy and methodology» (State registration number 117U002531); «Infocommunication aspects of economic security» (Protocol 1-20 of February 04,

2020, ISMA, Latvia), which emphasizes not only scientific but also practical focus.

The results of the research works presented in the joint monograph have a research and practice value.

The advantage of the joint monograph is the system and logic of the structure, the simplicity and accessibility of the material presentation, the presence of examples and illustrations.

We believe that the monograph will become one more step towards a scientific solution of the problems concerning the formation of an effective system of security management under trying circumstances of globalization.

Publication of the monograph «Security Management of the XXI century: National and Geopolitical Aspects» is scheduled to be annual. Currently, Issue 2 is offered to our readers.

With best regards,
Iryna Markina,
Honored Worker of Science and Technology of Ukraine,
Doctor of Economic Sciences, Professor,
Poltava State Agrarian Academy,
Ukraine

CONTENT

PART 3. THE MECHANISMS OF ENSURING ECOLOGICAL, FOOD, TECHNOLOGICAL AND ENERGY SECURITY IN THE DYNAMIC ENVIRONMENT

PART 4.INNOVATION ASPECTS OF FORMING SOCIAL,EDUCATIONAL AND INFORMATION SECURITY

ANALYSIS OF THE CYBER SECURITY POLICY OF UKRAINE

Oleksandr Chernonoh,
Master in Public Administration,
The General Staff of the Armed Forces of Ukraine, Kyiv, Ukraine,
Serhii Ivko,
Ph.D. in Technical Sciences, Senior Lecturer,
Poltava State Agrarian Academy, Poltava, Ukraine,
Artem Moskalenko,
Ph.D. in Technical, Head of Department, Poltava Institute of Business,
Private Higher Educational Institution Academician Y. Bugay
International Scientific And Technical University, Poltava, Ukraine

The issue of cybersecurity is increasingly ofted discussed at both national and international levels. Research findings from the publications indicate that nowadays most of the powerful countries in the world (NATO, USA, Russia, China, India and others) are in the process of transforming their own military capabilities having regard to opportunities of Internet use [1-3]. At the same time, cyberspace is gradually becoming a separate area of warfare activity, along with the traditional «Earth», «Air», «Sea» and «Space», in which the specialized cyber units of many countries of the world are increasingly active [4].

A special aspect of cyberspace, as the area of warfare space, is associated with the total digitization of both armaments and critical infrastructure of life support facilities. These realities have both a purely technological component and a human component: personal computers and smartphones of military personnel, computer equipment for navigating various drones, such as aircraft one; use of Supervisory control and data acquisition (SCADA) technologies; use of information and communication (ICT) technologies in all types of weapons – armored combat vehicles, planes, ships, missiles and even hand-carried weapons. The dependence of military technology on ICT increases each year, and therefore, the interchange of data between military ICT devices is an element of common cyberspace.

According to McAfee's CEO, released at the World Economic Forum in Davos in 2014, more than 20 countries have actually carried out various cyber operations in 2013-2014. Special units have been set up for: reconaissance in network, protection of own networks, blocking and «crash» of enemy structures. According to official statements, such units have been established in the United States, the United Kingdom (under the UK government), Germany, Australia, India and other countries. NATO, the leading international security organization, also takes an active role in cyber threat countermeasures.

The level of concern of the world's leading powers in the field of cybersecurity is evidenced by the desire to regulate the possibility of recognizing cyberattacks as an «act of war» of international standing. For example, in June 2013, an expert

group led by M. Albright proposed to interpret the large-scale cyber-attacks as cases falling under Article 5 of the North Atlantic Treaty and considered to be the attacks on all members of the Alliance. Such a position of NATO is also reflected in the new NATO Strategic Concept including the proposal to enhance NATO's organizational and military capabilities to counter cyber-attacks.

At the moment, in the context of the «hybrid aggression» of the Russian Federation, Ukraine has faced a critical situation, where the priority of national security is to ensure military security and defense of the state [5].

NATO defines hybrid warfare as a situation where a wide range of overt and covert military, paramilitary, and civilian measures are employed in a highly integrated design. One prominent leading theorist of hybrid warfare is F.G. Hoffman. Hoffman defines hybrid threat as, «Any adversary that simultaneously and adaptively employs a fused mix of conventional weapons, irregular tactics, terrorism, and criminal behavior in the battle space to obtain their political objectives» [6]. Hybrid war is a mixture of classic warfare with the use of irregular armed formations [7]. However, there are multiple diverse definitions for the same terms in different sources.

At present, the document defining the concrete content and practical mechanisms of the state's policy on ensuring military security is the Military Doctrine of Ukraine. However, the Law of Ukraine «On Organization of Defense Planning» defines the need to develop a Military Security Strategy as well, which is intended to determine the directions of prevention and neutralization of real and potential threats to the national security of Ukraine in the military sphere [8-9].

The military doctrine of Ukraine is a system of views on the causes, nature and spectrum of modern military conflicts, principles and ways of preventing their emergence, preparation of the state for a possible military conflict, as well as the use of military force to protect state sovereignty, territorial integrity and other important national interests [10].

Pursuant to the Constitution, Laws of Ukraine, National Security Strategy of Ukraine and the Military Doctrine of Ukraine, the Concept of Development of the Security and Defense Sector of Ukraine is put into effect, which defines a system of perspectives on the development of Ukraine's security and defense capabilities in the medium term, formed on the basis of the evaluation of security environment and financial economic capabilities of the state, implemented in the framework of a comprehensive review of the security and defense sector of Ukraine.

The provision of information security on the state level is currently based on the provisions of the National Security Strategy of Ukraine and the Doctrine of Information Security of Ukraine, approved in 2017 by the National Security and Defense Council of Ukraine (NSDC) decision.

Economic domain, scientific and technical area, information and public administration, defence industry complex, transport complex, electronic communication infrastructure, security and defense sector of Ukraine are becoming increasingly sensitive to the reconnaissance subversive activities of foreign spy

services in cyberspace. This is facilitated by the widespread, sometimes dominant presence of organizations, groups, individuals in the information infrastructure of Ukraine, which are directly or indirectly linked to terrorist and separatist movements predominantly widespread in Eastern Ukraine [11]. Modern information and communication technologies can be used for terrorist acts, in particular by violating the regular modes of operation of automated systems for managing technological processes at critical infrastructure facilities. Politically motivated cyberspace activity in the form of attacks on government and private websites on the Internet is becoming more widespread.

Increasingly, the cyberattacks and cybercrime are focused on information resources of financial institutions, transport and energy enterprises, government bodies that guarantee security, defense, and protection against emergencies.

The latest technologies are used not only for committing traditional types of crimes, but also for committing fundamentally new types of crimes common to society with a high level of information.

Cybersecurity threats are actualized by influence of the following factors:

- inconsistency of the electronic communications infrastructure of the state, the level of its development and security with the modern requirements;
- insufficient level of critical infrastructure protection, state electronic information resources and information against cyber threats, the requirement for protection of which is established by law;
- inconsistent cyber protection measures for critical infrastructure;
- insufficient development of the organizational and technical infrastructure for providing cybersecurity and cyber protection of critical infrastructure and state electronic information resources;
- insufficient effectiveness of subjects of the security and defense sector of Ukraine in counteracting cyber threats of military, criminal, terrorist and other nature;
- insufficient level of coordination, interaction and information exchange between cybersecurity entities.

Recent cyber-incidents and cyber-attacks on information and telecommunication systems of state information resources and critical infrastructure require high priority measures. For example, there were cyber-attacks with the use of malicious «Black Energy» software carried out on the energy industry objects, air transport networks of the «Boryspil» airport and rail transportation at the end of 2015 – beginning of 2016. About 30 institutions, including regional units of the Pension Fund of Ukraine, were hit and there were an unauthorized tampering to the Unified and State registers of the Ministry of Justice of Ukraine.

As a result of cyber-attacks, the network computer equipment of the State Treasury Service and the Ministry of Finance of Ukraine was disrupted on December 6, 2016, which resulted in failure of the treasury servicing of budget spending units and receivers (about 150,000 electronic transactions per day). During November-December 2016, there were about 125,000 cyber attacks in total detected, about

6,500 of them were targeted.

Investigation of these incidents indicates their involvement directly or indirectly with the security services of the northern «neighbor», which, by changing the tactics of «hybrid war», intensified aggressive actions in cyberspace by targeted cyber attacks, aiming at the destabilizing situation in Ukraine meaning the actual cyber warfare against Ukraine.

Today, the activities of the Russian APT 28 group, known as Fancy Bear, Sofacy, Sednit, Pawn Storm, or Strontium, are aimed at achieving the following goals:

- deliberate neutral positioning of the Russian Federation in the global information space, with the aim of positive conduct of future cyber wars;
- collecting information on cyber security systems of public authorities, military departments of the leading countries of the world;
- political and economic espionage;
- monitoring and regulation of the geopolitical situation with the help of fundamentally new technological principles and processes.

The activities of these groups are quite reasonably planned at a strategic and tactical level, which makes their behavior in cyberspace very covert and difficult to identify, unlike their Chinese counterparts.

The analysis suggests that we can expect an increase in cyber threats for the Ukraine. We must bear in mind that today cyber security sector is only partially ready to respond to massive cyber-attacks, that can be proven, in particular, by the scale of successful distributed denial-of-service (DDoS) attacks on government resources. A DDoS attack occurs when multiple machines are operating together to attack one target. DDoS attackers often leverage the use of a botnet - a group of hijacked internet-connected devices to carry out large scale attacks. Attackers take advantage of security vulnerabilities or device weaknesses to control numerous devices using command and control software. Once in control, an attacker can command their botnet to conduct DDoS on a target. In this case, the infected devices are also victims of the attack [12].

The appeal of some Ukrainian information security experts to create own cyber confrontation units indicate not only the level of attention to this problem, but the limited capacity of the state as well.

External players are actively preparing for large-scale cyber confrontations, changing their approaches to the vision of cyberspace, forming appropriate regulatory and organizational elements, heavily investing in it. Global geopolitical confrontation inevitably leads to an improvement in the quality of offensive cyber-weapons at the disposal of all geopolitical entities. It is not just the United States and China that are the spark plugs of the cyberweapon race, but also other powerful nations – Russia, India, the countries of Asia and the European Union. Ukraine cannot simply ignore this new reality, since further informatization processes will only prove that Ukraine's opponents (and possibly today's allies) have already moved from conditionally dangerous DDoS attacks to tougher actions – from cyber

espionage and cyber sabotage to conducting activities (operations) of military formations in cyberspace.

References:

1. The Verkhovna Rada of Ukraine Legislation of Ukraine. 2016. On the decision of the National Security and Defense Council of Ukraine of January 27, 2016 «On the Cybersecurity Strategy of Ukraine». [ONLINE] Available at: https://zakon5.rada.gov.ua/laws/show/96/2016. [Accessed 16 January 2020].

2. Chernonoh, O., Zhyvylo Y., Mashtalir V., (2015). Strategy for Cyber Security of the Armed Forces of Ukraine. Modern Information Technologies in the Sphere of Security and Defence, 3(24), 202-213.

3. Dubov, D. D. 2014. Cyberspace as a new dimension of geopolitical rivalry: monograph. Kyiv: The National Institute for Strategic Studies, 328.

4. Radkovets, Y., (2014). Signs of «hybrid war» technologies in Russia's aggressive actions against Ukraine. Science and Defence, 3, 36-42.

5. Magda, E. (2014). The Challenges of Hybrid War: An Information Dimension. Scientific notes of the Institute of Legislation of the Verkhovna Rada of Ukraine, 5, 138-142.

6. Vaczi, N. (2016). Hybrid Warfare: How to Shape Special Operations Forces. Master's Thesis. Fort Leavenworth, KS 66027-2301: U.S. Army Command and General Staff College.

7. Radio Liberty. 2020. The jacket is torn at the seam. [ONLINE] Available at: https://www.svoboda.org/a/2536203 1.html. [Accessed 20 January 2020].

8. Wilkie R. (2009). Hybrid Warfare. Something Old, Not Something New. Air & Space Power Journal, 23(4), 13-17.

9. Davis J. R. (2013). Defending Future Hybrid Threats. Military Review, 5, 21-29.

10. Legislation of Ukraine. 2020. About the National Security Strategy of Ukraine. [ONLINE] Available at: https://zakon.rada.gov.ua/laws/show/n0008525-15?lang=en. [Accessed 20 January 2020].

11. Puzyrenko O. G., Ivko S. O., Lavrut O. O., Klimovich O. K., 2015. Application of the information security risk assessment model in information and telecommunication systems. Information Processing Systems, 3(128), 75-79.

12. Official website of the Department of Homeland Security. 2019. Security Tip (ST04-015) Understanding Denial-of-Service Attacks. [ONLINE] Available at: https:// www.us-cert.gov/ncas/tips/ST04-015. [Accessed 20 January 2020].

Markina I., Aranchiy V., Safonov Y., Zhylinska O. and other. Security management of the XXI century: national and geopolitical aspects. Issue 2: [collective monograph] / in edition I. Markina. — Prague. — Nemoros s.r.o. — 2020. — Czech Republic. — 471 p.

Scientific publication

Security management of the XXI century:

national and geopolitical aspects. Issue 2

Collective monograph

In edition I. Markina, Doctor of Sciences (Economics), Professor

English language

Passed for printing 15.02.2020

Circulation 500 copies

ISBN 978-611-01-1814-9

Nemoros s.r.o.,
Rubna 716/24, 110 00, Prague 1
Czech Republic, 2020