JOURNAL OF SECURITY AND SUSTAINABILITY ISSUES
ISSN 2029-7017 print/ISSN 2029-7025 online
2020 March Volume 9 Number 3
https://doi.org/10.9770/jssi.2020.9.3(1)

ORGANIZATIONAL COMPETENCE OF NATO INFORMATION SECURITY POLICY

Mykhailo Loshytskyi[1], Oleksii Kostenko[2], Ihor Koropatnik[3], Galyna Tereshchuk[4], Vladyslav Karelin[5]

[1,2]National Prosecution Academy of Ukraine, 2a George Kirpy Street, Kyiv, 03055, Ukraine*
[3]Military Institute of Taras Shevchenko National University of Kyiv, 81 Mikhail Lomonosov Street, Kyiv, 03680, Ukraine
[4]Ternopil National Economic University, 11, Lvivska street, Ternopil, 46000, Ukraine
[5]Academy of the State Penitentiary Service, st. Goncha, 34, Chernihiv, 14000, Ukraine

E-mail: [2]koaduep@gmail.com (Corresponding author)*

Received 15 March 2019; accepted 10 January 2020; published 30 March 2020

Abstract. The science article is dedicated to the actual problem reinforcement and reformation the system of information security in counties that relate to the North Atlantic Treaty Organization. The main threatens to country's information security has been defined, the analytical grouping of problems by level of complexity and prognostication calamity have been made. The process algorithm for ensuring eternal operation of the information security system under the pressure of information threaten was elaborated. The critical components of NATO information infrastructure was well-defined.

Keywords: NATO; the information system; the information infrastructure; the information security system; interstate conflicts; national security; international cooperation

Reference to this paper should be made as follows: Loshytskyi, M., Kostenko, O., Koropatnik, I., Tereshchuk, G., Karelin, V. 2020. Organizational competence of NATO information security policy. *Journal of Security and Sustainability Issues,* 9(3), 735-746. https://doi.org/10.9770/jssi.2020.9.3(1)

JEL Classifications: F35, F42

1. Introduction

In today's conditions of distribution of political and military forces in the world, taking into account the construction of the information society, the actuality of organization the information security is raising - prevention and elimination by various means and methods of threats to the person, society, the state in the information sphere become more and more urgent. However, in today's multifaceted and dynamic world, information security problems are taking new features, now they go far beyond preventing wars and armed conflict.

2. Literature Survey

Today, they have become their foundation, first source, main resource and primary weapon. A volume research on country's information security policies and activity in the security aspect of the North Atlantic Alliance is presented in (Geers, 2011; Glyn, 2018; Kaija, Schilde 2014; Kempf, 2011; Shipan and Volden, 2008; Ključnikov, Mura, Sklenár, 2019).

Protecting their information interests, every state should take care of its information security. Also, it requires strengthening Ukrainian statehood. The balanced state information policy of Ukraine is formed as a part of its socio-economic policy, based on the priority of national interests and threats to the national security of the country. From a legal point of view, it is based on the foundation of constitutional state and is implemented through the development and realizing national doctrines, strategies, concepts and programs (Drobyazko et.al. 2019a, 2019b).

Aim of the study: To identify the main characteristics, the nature and dynamic of international cooperation on information security and to spot the features of the major problems of international cooperation, subjects and prospects of partnership between the North Atlantic Alliance country's.

3. Methods

Studying the issue of NATO's information security policy in modern conditions, above all it is necessary to explore the essence of the information policy of this organization generally, and also the issues of ensuring information security and cybersecurity in the Alliance system.

Now the regulation of the information field in NATO countries is implemented in the following areas:

1) promotion of competition, the fight against monopolism and concentration of the media;

2) ensuring the right and technical capabilities for access to information and information resources of the whole population;

3) observation of freedom of speech;

4) protection of the interests of national minorities, national cultural legacy, language, opposition to the cultural expansion of other countries; youth protection in the information sphere;

5) protection of intellectual property, the fight against piracy;

6) resistance to cybercrime; introduction of electronic management;

7) legal regulation of the Internet;

8) ensuring information security, etc. (Background information on the Alliance, its policies, activities and structures).

4. Results

The NATO information policy system is derived from the implementation of the democratic concept of civilian control over the military-political area in conditions of public participation in the international military-political process. In relation to increase in public interest in the activities of the Alliance in the early 1990s, the main role in production of information activities is assigned to NATO's own institutions. The main authority for the organization's information policy is the Atlantic Council, which publishes its decisions and statements to the press and the general public. Besides the Atlantic Council, the NATO-member countries are also involved in public informing.

One of the leading roles in realization the Alliance`s information policy is played by the Information and Press Bureau. It is one of the structures of the Secretary General's department (after the Prague Summit in 2002, it functions as the Department of Public Diplomacy, which provides information activities). Through the actualization of different programs and activities, the Information and Press Bureau helps partner nations and country- members to increase public awareness of the role and directions of NATO policies. The Bureau liaises with national information authorities and non-governmental organizations and arranges the events aimed at explaining public goals, missions and achievements of NATO (Background information on the Alliance, its policies, activities and structures).

NATO Information Security Issues

If we talk about ensuring the security of information, it should be noted that when NATO was created in 1949, the security systems of the member-countries differed considerably. The first NATO`s security system contained 8 levels of secrecy, was developed for documents in the form of "hard copies", and also covered for creating two central security agencies and a certain number of subordinate structures in every country . In the early 1990s, NATO began the political and military transformation of security structures, feeling not only positive (reducing exchange time, increasing carrier capacity, speed of search, classification, creating databases), but also negative (loss of confidentiality, integrity of information content or integrity systems, loss of access) consequences of informatization. The occurring of new threats in the information security sphere necessitated the modernization of attitude towards ensuring information security (Hughes, 2010).

The foundations of NATO's security policy for so-called classified information are set out in CM (2002) 49 The Security in the Organization of the North Atlantic Treaty (Document CV (2002) 49: Security within the North Atlantic Treaty Organization (NATO). Classified information - a term used in the legislation of NATO member-countries regarding "sensitive" information, that is to say, information, which is sensitive to threats, that arise from unauthorized access to it, and therefore needs to be protected or at least limit access. NATO has 5 levels of information security with limited access: Cosmic TOP Secret (CTS), NATO Secret (NS), NATO Confidential (NC), NATO Restricted (NR), Unclassified but Sensitive (North Atlantic Treaty Organization. Defending against cyber attacks).

At the same time, no more than 3 classification levels for information with limited access are used in innerstate legislation, including information with a stamp, which accords with the RESTRICTED level and refers to official and utility secrets. Certain terminological and substantive differences in the definition and classification of information with limited access in the national legislation of NATO countries are compensated by the unification of strategy to such information in the basic areas of activity of member states: military, economic, law enforcement etc.

Document CM (2002) 49 sets the basic requirements for a system for ensuring physical, organizational, procedural and technical security, including information security. Following cooperation obligations, each NATO member country provides information with limited access, own assessment, and, depending on how other members fulfill their obligations, defines which information they need to make available to the Alliance. Consequently, any deviation of one or several Alliance`s members from the fulfillment their obligations may lead to a volume reduction and quality of information passed them.

The document declares 5 basic concepts of NATO security policy:

1) amplitude;
2) depth;
3) centralization;
4) access control;
5) personal control (North Atlantic Treaty Organization. Defending against cyber attacks).

The ground concept of information security in NATO system is that information must maintain its grade of protection continually the entire cycle of its circulation, starting from the source. Furthermore, control over the distribution and extension of information has to excide its leak.

Tasks, related to information security, are the responsibility of NATO Internal Security Committee (NSC). This Committee is the deliberative authority to the Council on issues related to NATO security.

Inside NATO, the national authorized body for information security execute the functions of guiding the creation of a governing body and regime departments, providing the security of NATO secret information in all institutions under its jurisdiction, both inside and outside of the country, ensuring the development of information protection plans in case of emergence to prevent loss of confidentiality of NATO information. Representatives of the national authority for information security take part in meetings of the NATO Security Committee, where security policies and instructions proceed. On the capacity of the authorized representative body functions affects the size and quantity of the country's population, the geography of places where secret information is processed, and not least the distribution of powers between bodies in the sphere of national security. In some

NATO countries, the authorized body for information security is a part of the structure of the ministries of foreign affairs, defense and justice, in other countries it is headed by the Prime Minister or Minister of the Interior (NATO CCD CoE General Trends).

The country's accession to the PfP (Partnership for Peace) program envisages for the ratification of the Security Agreement between NATO and the countries participating in the EAPC (Euro-Atlantic Partnership Council) and / or PfP. According to the statements of this Agreement, the parties agree to consult on political and security issues, to expand and intensify political and military cooperation in Europe, realizing that the potency of cooperation in these areas involves the exchange of participants with secret information or other information with limited access. The responsible authority for protecting the information exchanged between the parties in cooperation under the EAPC/PfP is NOS. Moreover, between NATO and the partner-country concludes an agreement about mutual ensuring the security information, exchanged between the parties, and assigns a liaison officer between NOS and the national information security authority. All data exchanged between the parties under the EAPC/PfP are limited information and intended only for government usage. Unlike the standards for the protection of information adopted by the NATO system, the minimum norm for the processing and protection of classified information exchanged by the parties under the EAPC/PfP programs do not have a level of "top secret", because the amount of such information in the NATO system is utterly limited, and additional demands for ensuring the information security at this level of secrecy would unjustified tangle the mutual exchange procedure (NATO CCD CoE Mission and Vision).

This program uses the following information security support machinery:

– grants to establish and reinforce existing connection;

– creation of research centers;

– support for research projects.

The process of ensuring continuity of information security can be divided intsix main phases (Fig. 1).

Analyzing Figure 1, we can see that all stages are interconnected within the government system ensuring the information security. The public policy of supporting the country's information security defines the main directions of activity of authorities in this area. These directions are determined by the content of national interests, society and the individuals. In substance, that is true, as the task of information security measures is to minimize harm due to incompleteness, pastness or falsity of information or negative information impact due to the consequences of the functioning of information technologies, and also unauthorized extension of information. That is why information security assumes the presence of certain state institutions and the conditions of existence of its subjects, established by international and domestic legislation.

Review the basic building blocks (Figure 1)

Understanding the continual operation of information security system of the state. This phase is connected with the critical protection points (objects) identification. It is also about highlighting the main internal and external threats, that can become critical to the system.

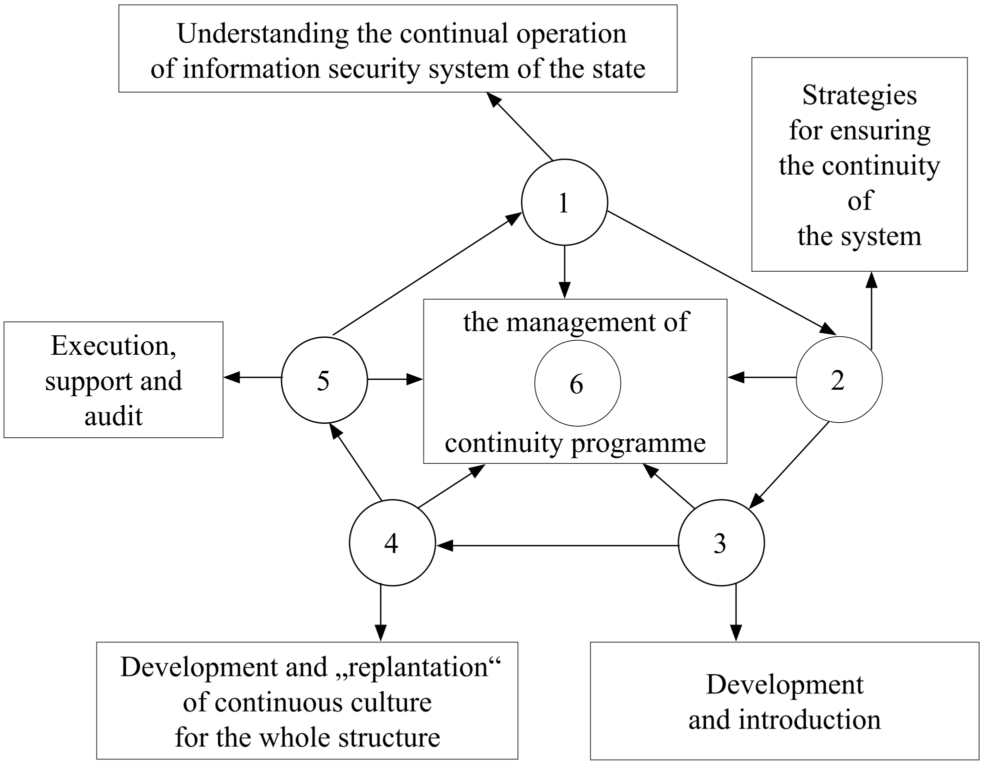
Understanding the continual operation of information security system of the state
Strategies for ensuring the continuity of the system
1
2
3
4
5
6
the management of
continuity programme
Execution, support and audit
Development and „replantation“ of continuous culture for the whole structure
Development and introduction

Figure 1. The process of ensuring the continuity information security system

Source: Designed by the authors

Strategies for ensuring the continuity of the system. In this case, the task is focused on identifying and selecting alternative solutions on demand of the system in order to minimize threats.

The search for solutions balances between the cost of protection systems and their effectiveness.

Development and introduction. In this phase, efforts are focused on structuring and documenting the Government Continuity Program.

The development of the state's information security culture provides for ensuring the process of development a state integrated information security system.

Execution, support and audit of the process of regulating the continuous functioning of the state's information security system in divers crises and conflicts.

The management of the state's information security program via the division of functions, provides for responsibility, insurance (guarantees) and management in the context of realization the general plan for the continual operation of the state's information security system.

Protection of the state information infrastructure

If damage is caused as a result of imperfect information relations, the use of low-quality information, etc., then it demonstrates a decrease in information security (NATO Cyber defense). This allows us to think of unsolved problems of ensuring the information security of NATO countries:

- imperfection of the information policy and information security policy of the state;
- imperfection of the legal framework in the field of information relations and information security;

– deficiently development of the information infrastructure of the state;

– illegal activity of officials, various formations and groups in the field of information interests of citizens and the state;

– imperfection of the state system for ensuring information security;

– the possibility of unforeseen circumstances in systems and processes, based on the usage of information technology.

– As a basic model of solving the information problem between two countries can be considered a pattern, which is based on the Richardson-Kasparov model (Madden, 2014). The pattern is based on the following conjectures:

– in the process of information attacks, each of the two countries tries to ensure the growth of the effectiveness of its information weapons proportionally to the level of the opponent;

– the economic potential of each country provides / limits the influence on the growth rate of the country's information capacities;

– States trigger an increase of the level of information capacities, guided by their own intentions.

We inject the signs N1 (t), N2 (t) of the information power levels for each part of the conflict, where t - time. Then, the above conditions for the model operation can be formalized in the form of a system of two ordinary differential equations:

$$\dot{N}_1 = M_1(L_1 - N_1) \text{ x } [1 - \exp(-p1(k_1N_2 - a_1N_1 + g_1))]$$
$$\dot{N}_2 = M_2(L_2 - N_2) \text{ x } [1 - \exp(-p2(k_2N_1 - a_2N_2 + g_2))], \qquad (1)$$

where M_1, M_2 , L_1, L_2, p_1, p_2, a_1, a_2, k_1, k_2 are positive coefficients, independent of time.

The parameters of model (1), by analogy with T. Saati, are defined as follows:

k1, k2 - reaction indexes of information attacks;

a1, a2 - costs indicators for the generation of information weapons;

g1g2 - pretence (aggressiveness) indexes if they are positive, or goodwill indexes if they are negative;

M1, M2 - the cost of available information support;

L1, L2 - limit values of information power levels;

p1, p2 -indexes of importance of information costs.

Model (1) admits the existence of four special solutions, that determine the coordinates of the balanced positions:

$$1)\ N_1^p=N_1^*,\ N_2^p=N_2^*,\quad 2)\ N_1^p=N_1^*,\ N_2^p=L_2\quad 3)\ N_1^p=L_1^*,\ N_2^p=N_2^*,\quad 4)\ N_1^p=N_2^*,\ N_2^p=L_2 \qquad (2)$$

where N1 * N2 * is a solution to a system of linear algebraic equations.

The functions $u_1 = r_1^0(x_1 - x_2)$ i $u_2 = r_2^0(x_2 - x_1)$ characterize the policy of each country in the field of information opposition, where the variables $x_1 = N_1 - N_1^*$; a $x_2 = N_2 - N_2^*$ have excursion from the equilibrium levels of information power. Here r_1^0, r_2^0 are stationary control parameters. Given the form of the function u_1, u_2 system (1) takes the form:

$$\dot{x}_1 = M_1 \text{ x } (\delta_1 - x_1) \text{ x } [1 - \exp(p_1(a_1x_1 - k_1x_2))] + r_1^0(x_1 - x_2)$$
$$\dot{x}_2 = M_2 \text{ x } (\delta_2 - x_2) \text{ x } [1 - \exp(p_2(a_2x_2 - k_2x_1))] + r_2^0(x_2 - x_1) \qquad (3)$$

The following conclusions can be made: each state, is a part of the global information space, must formulate a system of measures for its own steady information development in conditions of fierce competition, taking into account information security factors. To do this, you need to:

– understand the information attacks and how to opposite them.

– create the software to oppose the information attacks;
– analyse information threat indicators to improve decision-making mechanisms in public administration systems;
– assure the highest protection against exterior impacts;
– analyse and technical audit of all means of communication;
– consolidation of the activities of public authorities and Mass media in the field of political public awareness in order to neutralize the negative psychological effect in crises and conflicts (Kasapoglu, 2015).

One of the important task of NATO is to prevent acts of aggression in cyberspace, because cyber attacks become more frequent and more organized, and losing for government agencies, enterprises, objects of critical infrastructures, and also can reach a critical level that menaces to national and Euro-Atlantic prosperity, security and stability of the entire world community. Foreign military and intelligence services, organized criminal groups, terrorist and / or extremist groups can be the source of such attacks.

NATO Information Security Management

Despite the fact that NATO has been constantly protecting its information systems since its formation, at the Prague Summit in 2002, this issue was put into the political circle. Taking into account the technological progress achieved after the Prague Summit, the leaders of the Alliance countries at the Riga Summit in 2006 again assumed the need to ensure cyber security. At the same time, before the cyberattacks in Estonia in 2007, NATO's activity in the cyber defense area focused mainly on protecting communications systems owned by the Alliance and were used by its members. The cyber attacks of 2007 forced NATO to think seriously about the problems of ensuring the cyberspace security, especially, to perceive the threats incoming from the Internet space as strategically important. NATO conducted a meticulous assessment of its approach to cyber defense and in October 2007 a report, based on that appraisal, was prepared to defense ministers of member-countries with recommendations on specific tasks of NATO, new sanctions to improve protection against cyber attacks. The official NATO Cyber Defense Policy was favoured by the defense ministers of the Member States and presented to the organization in April 2008 at the summit in Bucharest. The aim is "to provide opportunities to support allied countries, on demand, in resistance to cyber attack" (Nečas, Andrassy, 2018).

The number and complexity of cyber attacks increased quickly after the attacks on Estonia in 2007, and in the summer of 2008, the Russian war against Georgia had shown that cyber attacks became one of the main part of military operations using traditional weapons. Therefore, at the Lisbon Summit of NATO in 2010, was decided to develop a new organization's policy of cyber defense, as well as a specific plan, which came into operation in June 2011. As part of their realizing, NATO uses defense planning processes to protect allies from cybercrime, and to optimize interaction, collaboration and information exchange. NATO works closely with the EU and the UN (Smaliukiene, 2018) on resistance to cyber threatens issues.

The future security of the NATO depends on the fast development and constant complication of cyberattacks, which The Strategic Concept and the Declaration of the Lisbon Summit have noted. The information attack is one of the most dangerous act of provocation and threat to the security and prosperity of the member states of the alliance. In the hierarchy of provocations, listed in this concept, dangers, that come from the information space, located immediately after the propagation of weapons of mass destruction and terrorism. Such attention, particularly, to the phenomenon of securitization due to which cybersecurity "has evolved from a technical discipline into a strategic concept".Today, NATO is developing tools to prevent, detect, react and recover from attacks using the created Cyber Security Authority, the Common Center for Excellence in Cyber Threat Protection, and the Computer Emergency Response Force (National Cyber Security Strategy: Securing our Digital Future).

The Cyber Security Management Authority (OCHA) is responsible for agreement cyber protection activities inside of the organization. NATO CIDO is ran by the Cyber Defense Management Commission, which includes the leaders of NATO's political, military, operational and technical authorities responsible for cyber defense issues.

It is the main consultative body of the North Atlantic Council on Cyber Defense and counsel some aspects of cyber defense to member countries. NATO CSTO is a part of the NATO Headquarters Security Challenge Office. The Center for Excellence in Cyber Defense (Tallinn), which received NATO accreditation in October 2008, is not given operational functions and acts as an instructional and training center where doctrinal and conceptual foundations of cybersecurity are elaborated. It is positioned as "the main source of expertise in the cyber defense field", which "accumulates, creates and spreads knowledge on key cybersecurity issues within NATO, between the Alliance states and its partners" (Petrauskaitė, Rusko, 2018).The center carries out research and training on conducting information operations in the virtual space. With the support of the Civilian Communications Systems Planning Committee, the Center for Excellence in Combating Terrorism (Ankara), and the NATO "Science for Peace and Security" Program, the Center for Excellence in Cyber Defense conducts expert negotiations, seminars and exchanges of information with interested partners and international organizations (for example, with the EU and the OSCE). In 2015, the Center published a book on cyber war of Russia against Ukraine titled "Cyber War in Perspective: Russian Aggression against Ukraine", which analyzes current acts in the field of information protection and the strategic and tactical aftermath of cyber war. On the pages of this issuance, experts, especially, note that the term "cyber attack" includes digital propaganda, DDoS campaigns, website defenses, leak of information due to attacks, and usage of malicious software for spying (Börzel and Risse, 2009). British experts reckon OCHA and the Tallinn Center as elements of a single organizational system, where the first is endowed with "wide facilities for real-time electronic monitoring" and functions at the operational-tactical level, while the Center, elaborating the long-term doctrine of NATO, constitutes an "intelligent platform" and is an element of a strategic level. Currently, the Center's experts are finding the militarization of the Internet as one of the most dangerous trend in the global cyberspace (Glando, 2013).

As a result of the Warsaw Summit of Heads of State and Government participating in the meeting of the North Atlantic Council in July 2016, a released statement notes that cyber attacks are an obvious security challenge for the Alliance and can be not less destructive for modern societies than usual weapon attacks. Accordingly, cyber defense is one of NATO's main mission - collective defense, and cyberspace is considered as a field of operations, where NATO defends itself as effectively as it does in the air, on land and at sea. This will increase NATO's ability to defend and conduct operations in these areas, conserve freehand and decisions in different circumstances, and will promote NATO with provision of wide deterrence and defense capabilities.

NATO is cultivating cooperation with cyber defense in conformity with the Instructions on Cooperation with Cyber Defense with Partners and International Organizations 2008 and the Framework Document for Cooperation with Cyber Defense of NATO and Partner Countries in 2009, accepting the need to define united approaches for using modern information protection systems, in view of information security requirements. Information security in the case of creation common information and telecommunication systems, where information with limited access circulates, is achieved through the development of offers of the protection of confidential communications using NATO equipment, that is necessary to create information and communication systems in government, along with upgrading their specialists regarding the Information Security within PfP (Cornish, 2014).

The terminological base, used at the EU level is reflected in the EU Council Directive "about European Critical Infrastructures and Measures for Their Protection". The critical infrastructure in this document is presented as "tools, systems or a part of them, located in the EU countries, having importance for maintaining vital public functions, health, safety, defense, economic and social welfare of the people and the failure of which or even destruction will cause serious consequences for EU member states due to the above functions fail". In the information sphere, civilian and military objects are bound up (Reynolds, 2007). Table 1 compares the Russian and American sight of critical state infrastructures.

Table 1. Critical Information Infrastructures of EU and US Countries

EU countries	USA	Military / Civilian sphere of application
Healthcare	Public health	Civilian objects
-	First Responder Services	Civilian objects
-	National monument	Civilian objects
Agriculture	Feeding and Agriculture	Dual-use facilities
Water supply		Dual-use facilities
Public administration	Public administration	Dual-use facilities
Large scale Information systems		Dual-use facilities
Information and telecommunication systems	Information and telecommunication systems	Dual-use facilities
Energy industry	Energy industry	Dual-use facilities
District heating	-	Dual-use facilities
banking and financial systems	banking and financial systems	Dual-use facilities
Transport system	Land and maritime transport	Dual-use facilities
Industry	Critical production	Dual-use facilities
-	Post Service	Dual-use facilities
Municipal management	-	Dual-use facilities
Civil defense	-	Dual-use facilities
	Military-industrial complex	Military aim
Defense		Military aim

Source: Developed by the authors according to the source The World Factbook: Central Intelligence Agency

Currently, critical information and traditional infrastructures exist. However, subject to the formation of the "digital economics" there is observed a wide spread of information infrastructures, because they are more economical, efficient and ergonomic.

NATO also comprehends the need to strengthen monitoring of critical networks within the Alliance and preclude identified drawbacks. For that purpose, the Tallinn Center organizes tuition and assists member countries in improving cyber defense programs, and the allies expand their early prevention resources in the form of a common network of monitoring nodes and sensors. NATO uses the defense planning process to promote the development of cyber defense capabilities of allies, helping individual member countries and optimizing information exchange, cooperation and compatibility (Quackenbush, 2015).

5. Discussion

In relation to increased danger of cyber attacks, NATO sets the requirements for all countries, interested in maintaining the integrity, inviolability and confidentiality of their information space. Especially, the information structure of the Alliance member countries should be constantly improved, development rate of the recent information technologies and their extension should accelerate. The development of electronic certification systems, cryptography, proper training of personnel are also needed. The formation and implementation of a unique state policy in the context of ensuring the security of national interests from threats in the information field should be one of the priority areas for the development of every state. The industry development of information and telecommunication facilities, their distribution in the domestic media market, the modernization of telecasting and broadcasting systems, the updating of the technical base to ensure the protection of information are also important steps to assure information security.

As a result of attacks, directed against government and implemented through the Internet, NATO's attention has pointed towards the issue of cyber defense of individual member countries. The Alliance does not exclude the need to respond quickly to cyber attacks by sending a team of experts to any member country that suffers from cyber attacks, or to a country that feels the measure of invasion of its information space. Nevertheless, one of the main role in protection and security of their own communication systems signify the allies themselves. NATO requires a reliable and secure auxiliary infrastructure, therefore continue to work with the national authorities to develop concepts and criteria for ensuring a minimum level of cyber defense where national networks and NATO networks are interconnected (Linke & Zerfass, 2011).

In course of time, NATO plans to completely provide itself with an appropriate set of cyber defense tools, including passive and active elements. NATO also works closely with other organizations to overcome the security risks in cyberspace.

The issue of ensuring information security of NATO, besides the technical support and strategic planning issues, also has a political measuring. First of all, it involves the possibility of applying the Article 5 of the Washington Treaty in information attacks. The main protagonists of expanding the concept of collective liability in the field of ensuring information security in the NATO system are Estonia and the United States. Particularly, Professor J. Goldgeyer notes that, cyberattacks are not an “armed attack”, so, they are not refer to Art. 5, anyway, we can draw a conclusion that the Alliance “must unify to resist attacks, which menace the security of any member of NATO”.

Notably, the issues of countering threats to information security, including cybersecurity, belong to “soft security” field, while NATO’s main task is resistance to convention security challenges - provision “hard security”. Therefore, another topical factor that displays itself at the transatlantic level is the “division of labour” between NATO members hence some countries specialize in “soft security”, while others carry “solid” military missions. The consequence of this is a difference in resistance approaches: the USA, France, Great Britain and Germany compare the information security with military strategy, but Estonia, which does not have a powerful military potential, emphasizes the key role of civil society and the private sector.

Conclusions

Based on the analysis of the current legislation and practice of European countries, it is proposed to refuse the legislative fixing list of information security threats. Agreeably, it was offered to provide at the same time, firstly, information security from demolition, distortion, blocking, unauthorized leakage or infraction of the set routing procedure, and secondly, information security of the citizen and society. This requirement is dictated by the value of the information picture of the world, which is formed by the individual and social levels. A common tool of threats is the spread of the so-called N. Pathogenic texts aimed at deconstructing ideological, value, moral and ethical and other mental systems.

It is proved, that opposition information threats mechanisms from external sources should include:
a) the ensuring security purpose, concludes in maintain the integrity and security of the information sphere in the process of its functioning;
b) the level of security, that identifies the elements of the system that may face potential and real hazards;
c) security sector, that defines the functioning and development of the information sphere;
d) security parameters, that set the allowable limits of deviations in the information security system potential, the quantity of its elements, their quality, connection;
e) a list of threats, the consequences of their realization and prevention mechanisms.

The methods of resistance to information threats from external sources are provisionally divided into 2 groups:
1) preventive - are used to avoid the deployment of threats or to prevent the appearance of new risks on the entry-level of forthcoming such threats;
2) operational - are used directly in reply to the aggressive steps of external sources of information threats and related to their launching and realization.

The necessity of developing the functional duties of the subjects of ensuring information security of NATO countries in relation to the implementation of coordination and interaction is proved.

References

Background information on the Alliance, its policies, activities and structures. Available on the Internet: http://www.nato.int/cps/en/natohq/topics.htm

Börzel, T.A. and Risse, T. (2009). The transformative power of Europe: the EU and the diffusion of ideas. KFG Working Paper Series, No. 1, May. Berlin: Freie Univ.

Cornish, P. (2014). Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks. Brussels: European Parliament

Document C-V (2002) Security within tne North Atlantic Treaty Organization (NATO). Available on the Internet: http://www.statewatch.org/news/2006/sep/nato-secclassifications.Pdf

Drobyazko S., Okulich-Kazarin V., Rogovyi A., Goltvenko O., Marova S. (2019). Factors of Influence on the Sustainable Development in the Strategy Management of Corporations. Academy of Strategic Management Journal. Volume 18, Special Issue 1 (Title: Strategic Research Directions), 2019. URL: https://www.abacademies.org/articles/Factors-of-influence-on-the-sustainable-development-in-the-strategy-management-of-corporations-1939-6104-18-SI-1-439.pdf

Durmanov, A., Bartosova, V., Drobyazko, S., Melnyk, O., Fillipov, V. (2019b). Mechanism to ensure sustainable development of enterprises in the information space. Entrepreneurship and Sustainability Issues, 7(2), 1377-1386. http://doi.org/10.9770/jesi.2019.7.2(40)

Geers, K. (2011). Strategic Cyber Security/ K. Geers. – NATO Cooperative Cyber Defence Centre of Excellence

Glando, B. D. (2013). Cyberspace Warfare: A New DoD Core Mission Area (No. ADA581106). National Defense University Joint Advanced Warfighting School, Norfolk. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a581106.pdf

Glyn, B. (2018). How digital media reshapes political activism: mass protests, social mobilization, and civic engagement. Geopolitics, History, and International Relations 10(2): 76–81.

Hughes, R.B. (2010). NATO and Cyber Security: Mission accomplished? Available at: http://www.carlisle.army.mil/DIME/documents/NATO%20and%20Cyber%20Defence.pdf

Kaija, E. Schilde (2014). Cosmic top secret Europe? The legacy of North Atlantic Treaty Organization and cold war US policy on European Union information policy, European Security http://doi.org/10.1080/09662839.2014.911175

Kasapoglu, C. (2015). Russia's Renewed Military Thinking: Non-Linear Warfare and Reflexive Control (Vol. 121). NATO Research Division - NATO Defense College. Retrieved from https://www.files.ethz.ch/isn/195099/rp_121.pdf

Kempf, A. (2011). Considerations for NATO Strategy on Collective Cyber Defense Available at: http://csis.org/blog/considerations-nato-strategy-collectivecyberdefense

Ključnikov, A., Mura, L., Sklenár, D. (2019). Information security management in SMEs: factors of success. Entrepreneurship and Sustainability Issues, 6(4), 2081-2094. http://doi.org/10.9770/jesi.2019.6.4(37)

Linke, A., & Zerfass, A. (2011). Internal communication and innovation culture: developing a change framework. Journal of Communication Management, 15(4), 332-348.

Madden, D., Hoffmann, D., Johnson, M., Krawchuk, F., Peters, J. E., Robinson, L., & Doll, A. (2014). Special Warfare. The Missing Middle in U.S. Coercive Options. Santa Monica, Calif.: RAND Corporation, RR-828-A. Retrieved from https://www.rand.org/pubs/research_reports/RR828.html

Nečas, P., Andrassy, V. (2018). Diplomatic Missions' Order versus Security and Sustainability, Journal of Security and Sustainability Issues, 8(2), 267–276. https://doi.org/10.9770/jssi.2018.8.2(13)

North Atlantic Treaty Organization. Defending against cyber attacks. Available on the Internet: http://www.nato.int/cps/en/natolive/topics_49193.htm

NATO CCD CoE Mission and Vision. Available on the Internet: http://www.ccdcoe.org/11.html

NATO CCD CoE General Trends: [Online tool]. – Available at: http://www.ccdcoe.org/8.html

NATO Cyber defence. Available on the Internet: http://www.nato.int/cps/en/natohq/topics_78170.htm

National Cyber Security Strategy: Securing our Digital Future. Available on the Internet: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM: 20090149:FIN:EN:PDF

Quackenbush, S. L. (2015). Centers of gravity and war outcomes. Conflict Management and Peace Science. https://doi.org/10.1177/0738894215570430

Reynolds, C., (2007). Governing security in the European Union: institutions as dynamics and obstacles. In: Dirk de Bièvre and Christine Neuhold, eds. Dynamics and obstacles of European governance. Cheltenham: Edward Elgar, 51–76.

Shipan, C.R. and Volden, C. (2008). The mechanisms of policy diffusion. American journal of political science, 52 (4), 840–857.

The World Factbook: Central Intelligence Agency. Available on the Internet: https://www.cia.gov/library/publications/the-world-factbook/fields/2144.html

Von Hippel, E. (2005). Open source software projects as user innovation networks. Perspectives on free and open source software, 267-278.

Short biographical note about the contributors at the end of the article:

Mykhailo LOSHYTSKYI, Doctor of Law, Professor, Honored Worker of Science and Technology of Ukraine, National Academy of Legal Sciences of Ukraine
ORCID ID: orcid.org/0000-0003-2127-6935

Oleksii KOSTENKO, Research Institute of Informatics and Law of the National Academy of Legal Sciences of Ukraine
ORCID ID: orcid.org/0000-0003-2535-4839

Ihor KOROPATNIK, Doctor of Science of Law, Assotiate Professor, Military Institute of Taras Shevchenko National University of Kyiv
ORCID ID: orcid.org/0000-0002-0493-0710

Galyna TERESHCHUK, Candidate of Juridical Sciences, Ternopil National Economic University
ORCID ID: orcid.org/0000-0003-0548-0920

Vladyslav KARELIN, Candidate of Juridical Sciences, Academy of the State Penitentiary Service
ORCID ID: orcid.org/0000-0002-6271-2447

Register for an ORCID ID:
https://orcid.org/register