FOLIA 313

Annales Universitatis Paedagogicae Cracoviensis

Studia de Securitate 10(2) (2020)
ISSN 2657-8549
DOI 10.24917/26578549.10.2.2

Iryna Patlashynska
ORCID ID 0000-0002-8551-5956

Lesya Ukrainka Eastern European National University

The international experience of the information security of the nation

The relevance of the study

In the modern world, information security plays an important role in the context of the globalization of the information society. The constant informatization of the sphere of security of the individual, society, economy and finances, and national infrastructure highlights the need for a comprehensive approach to the problem of information security, which has become especially important today. Further, the protection of the state's information and media field is closely related to the concept of information security, which can be considered to be the protection of inside information. As such, it implies the security of the quality of information, its reliability, the protection of national, banking, and commercial secrets from disclosure, and the protection of the nation's information resources.

It is important for the nation's information security to achieve a state of security, that is, to create and maintain appropriate engineering and technical facilities and information organization that meet real and potential threats, as well as to consider the demographic and economic situation of the country. Information security issues are relevant to all nations to some degree. However, the specific weight of engineering, hardware, and software methods of national security in different countries varies and depends on a complex set of conditions related to the potential internal and external threats, relations with neighboring states, and geopolitical centers.

The analysis of recent publications

The problems of the protection of the media and information spheres of the nation and information security, in general, have been considered in the research of both

native and foreign scientists, including: G. Vynogradova, V. Zdorovega, O. Kopylenko, V. Lyzanchuk, V. Myronchenko, A. Moskalenko, G. Pocheptsov, V. Rizun, A. Chichanovskiy, V. Shklyar, V. Vorobyov, T. Dobroskolonskaya, K. Markelov, L. Mohammedova, V. Popov, O. Gritsenko, S. Chukuta, I. Aristova, V. Bogush, O. Dubas, V. Kravchenko, O. Lytvynenko, Ye. Makarenko, G. Nesvit, O. Oliynyk, O. Sosnin, O. Starysh, and O. Yudin.

V. Lyzanchuk, a well-known expert in the field of mass communications, states:

> (…) human communities are created by networks of information communications, through which the necessary state-political, socio-economic, ideological, historical, ethnic and other information is transmitted. The national media network is one of the 'three whales' on which nation consciousness is based, along with the national intellectual class and the national political elite[1].

However, media organizations are not only able to consolidate society but also to play a destructive role, undermining its social and psychological stability by creating and promoting negative values, alien to the national culture of ideals and values in the mass consciousness. Therefore, society and the state must constantly try to neutralize the regressive tendencies in the information-axiological field and mobilize the resource potential of the media for the formation of a value system that could ensure the spiritual unity of the society and information security of the nation.

This problem is particularly relevant today for any nation facing the task of consolidating society into a single political nation with a high level of national consciousness. As the information activities of the mass media continue to grow and intensify, affecting all aspects of society and the nation, the task is to ensure that these activities are in accordance with the national interests of the state. Therefore, the study of the information security of the nation in the context of the tools of mass media influence on the formation of national consciousness is appropriate and timely.

The purpose of the present study is to analyze the importance of national information security in the context of global information impact.

The main body of the research

From early childhood, people are surrounded by information – they cannot live without information and perceive it through many channels. It is by processing this information that they shape their behavior. The media creates a kind of information world in which a person, particularly a young person, produces a certain outlook on life, lifestyle, way of living, types of behavior, etc. However, as was noted, media information is mostly unsystematic and sometimes contradictory.

Mass media reflects people's living conditions, the system of their connections, and their dependencies on a macro and micro scale. Thus, mass media performs two

[1] V. Lyzanchuk, *The phenomenon of the immortality of the war*, "Scientific Notes of the Academy of Sciences of Ukraine" 2004, Iss. 6, pp. 74–81.

seemingly opposite tasks: it captures and develops the interests of both individuals and society. The political, social, and psychological aspects of the media phenomenon are difficult to separate. There is a clear correlation between social and psychological approaches to a common goal. Technical means disseminate information that contains specific ideas to shape (or influence) people's attitudes, evaluations, opinions, and behavior. Often, in this case, mass media performs not so much information and cultural functions, but ideological ones.

Mass media's multidimensional penetration into society can play both a unifying role, contributing to the consolidation of society, and a disintegrative, separative role, introducing negative stereotypes into the public consciousness. According to G. Blumer, this is especially noticeable in the development of a crisis, when people who feel social uncertainty are particularly influenced. They easily respond to various new stimuli, ideas, and they are more exposed to propaganda and manipulation[2].

In addition, public media is often associated with "public communications" and may take many forms. Thus, it can relate to different groups of people and be associated with many different directions. At the same time, public media is a means of creating discussion and engaging ordinary citizens, united by certain goals. The main feature of public media is that it is independent of commercial trends and popular topics for discussion. This makes it possible to create different public media models that may offer open editorial policies or be more focused on involving the citizens in media[3].

Because it uses alternative channels of information, modern media should have approximately the same potential to influence the public (popularity, level of trust, etc.). In this case, the number of foreign information companies operating in the territory of the state does not matter – their influence will be adequately balanced by the activities of native ones. Conversely, in the case of low-power native information resources, there is the possibility of complete information isolation of entire regions or even states through foreign media activity.

Most often, US CNN and the British Air Force have the right to cover the news for the world community (for example, during the US Army invasion of Panama in December 1989–January 1990, the Desert Storm combined joint operation in Kuwait and Iraq in 1991, the US Army invasion to Haiti in 1994, the NATO forces operations against Yugoslavia in 1999, Afghanistan in 2001, and Iraq in 2003).

During the Velvet Revolution in November 2003 in Georgia, the events in Tbilisi were under constant attention from the Georgian and foreign media (which played a special role). On November 22, 2003, the day the Georgian Parliament was captured by force, CNN broadcasted a live five-hour report from the venue[4].

[2] V. Badrak, *Factors of effectiveness of influence of mass media on electorate*, extended abstract of Doctor's thesis, KNU 2000, p. 23.

[3] O. Dika, *Information warfare. Modern tendencies of web communication*, http://webstyletalk.net/node/97, [accessed: 20.10.2019].

[4] S.I. Hrynyayev, *Information war: History, today and outlook*, http://www.4.narod.ru/warfare/grinyaev/page009.htm, [accessed: 20.10.2019].

It should be noted that Georgia does not have a powerful media of its own that could compete with the global media giants. Therefore, the meticulous attention of the world community to the transformations in the North Caucasus was of double importance.

On the other hand, the events in Georgia could be a classic example of a special information operation with wide use of media opportunities and NGOs, generously funded by foreign states. Today, any version is of these events is possible, but regardless, it is a clear example of the consequences of underdevelopment of the information space of the state.

The social norms, aspirations, needs, and public opinion existing in society are largely shaped by the media. By communicating with the consumers of their products, television, radio, internet, etc. brought all the inhabitants of one "global settlement" closer, providing the opportunity not only to get to know each other better but also to become informed about the same topics at the same time. This process has one key characteristic: communication, as well as the nature of information, is one-sided. We have the right to trust or not trust the information we have received, but we cannot argue with the television or the newspaper for the same reason that we do not speak with the trolley. The column "letters to the editor" does not correct this shortcoming, since only a small part of information consumers become involved in the discussion, and the inappropriateness of publishing all the letters allows editors to choose only those that correspond to the views of the media.

All consumers of information individually process the same facts through the media. However, the peculiarity of modern media (and especially the most common and effective ones – television and radio broadcasting) is that information is not transmitted in the form of facts but as ready statements, conclusions, and analytical materials. The consumer is deprived of the opportunity to discuss with the "opponent" and most often simply accepts the high quality prepared material from authoritative sources. Discussion is not public in a communicative (not legal) sense – consumers receive information personally.

Therefore, this is a one-sided dialogue: the media is convincing. A classic example is the situation during the 1930s in London and New York when "The War of the Worlds" by Herbert Wells was broadcasted for the first time. The population of these cities began to panic because of the imaginary invasions of Martians[5].

Thus, a team of specially trained media professionals, carefully selected experts, and analysts opposes the mind, experience, and wisdom of a single media consumer. At the same time, the basic mass of the information that makes up a person's experience was not received directly but through the same media. As a result, the process of thinking is unified and collectivized, and the phenomenon of "collective solidarity" arises when one has to approve or condemn certain events in society.

[5] N. Gurina, *Information confrontation as one of the main directions of the policy of modern international intercourse*, http://www.experts.in.ua/baza/analitic/index.php, [accessed: 20.10.2019].

For example, in May 2005, a huge wave of violence and spontaneous protests stirred the Muslim world. According to official data (which was leaked to the press after American censorship), fifteen people were killed and more than seventy people injured during the repression of protests in Afghanistan. The driving force behind the riots was the information published in the British Newsweek about the US Naval Station Guantanamo Bay (a detainment center for those connected with al-Qaeda), where the desecration of the Quran had been observed[6].

The destructive influence on the existing system of values (a symbolic system) in society is realized primarily through information and media as universal channels of transmission. A key role in the destruction of the Christian values of Ukrainian culture was played by the promotion of violence, cruelty, and immorality. It is yet another matter that the countries of Western democracy have also faced similar problems. This trend can be seen as an undesirable but integral part of liberalization. Thus, we cannot say that it is a deliberate influence of western special services (or any other)[7].

Accordingly, at the micro-level of the information security of the nation, the role played by the media in resolving a particular conflict depends on the extent to which journalists are free in their professional activities and how open their access to important public information is[8].

According to S. Neklyayev, the media's special attachment to any currents, parties, leaders, or financial groups is particularly active during extreme events and armed conflicts at the macro level of the nation's information security.

> A massive attack on public opinion begins, complex mechanisms of influence are applied – from simple counterarguments to multi-level refutation, which is based on the analysis of facts and statistics, the evaluation of events through the opinions of personalities, authoritative experts. Media uses agents of influence and counter--influence, work to block and neutralize information flowing through alternative channels to lobby the interests of the group to which they belong or sympathize[9].

The media can weaken or, alternately, to strengthen certain emotions and feelings. H. Ibraieva believes that the professional management of providing news on live broadcast can lead to the limited, sterile perception of murder and suffering.

> The most important is that the technology of communication and electronic weapons allow the enemy to deal devastating blows in an extremely short time. The Persian Gulf War was the general rehearsal of a new type of war, and its 100-hour process, during which the Allies defeated a large and well-armed Iraqi army, was

---

[6] S.I. Hrynyayev, *Information war*…, op. cit.

[7] O.K. Yudin, V.M. Bogush, *Information security of the nation*, MK-Press 2005, p. 576.

[8] G. Blumer, *Collective behaviour* [in:] *American Sociological Thought. Texts*, D. Vodotynskogo (eds.), Izd-vo MGU 1994, p. 278.

[9] N. Gurina, *Information confrontation*…, op. cit.

a demonstration of the resolve of the new military powers during the solution to an important issue (in this case, oil delivery to the West)[10].

Thus, in the early 1990s, the term "Information War" began to be used to denote the possibility of influencing society through a certain way of presenting news and information in order to form the "right" opinion. The concept was defined as the following: "Use and management of information to gain a competitive advantage over an adversary in a conflict". The term was used by the US Department of Defense and subsequently became more widespread and more meaningful[11].

For the first time, this concept was enshrined in the US Department of Defense's DOD S 3600.1 directive (December 21, 1992), where it was used narrowly and considered as a form of electronic warfare. Subsequently, in the report of the American Rand Corporation MR-661-0SD Strategic Information Warfare. A New Face of War (1996), the term "strategic information warfare (information warfare)" appeared for the first time. It meant war using the state's global information space and infrastructure to both conduct strategic military operations and strengthen its influence on its own information resource. The very concept of "information war" existed and has been used for a long time. There were efforts to influence conflict through information and media even during World War I[12].

D. Volkogonov notes that during World War I, the corresponding departments and units, which organized the "War of Words" (the agitation of the enemy), were created within the army headquarters.

England was the most active in the War of Words, using printed cards to disseminate information. More than a million of these cards were dropped from air balloons flying over the enemy's location. The British government created special administrative bodies to provide the printed press of other countries with British versions of the war. In the "War on Illustrations", newsletters were published, and military films about the situation at the front were made[13].

Germany also tried to wage a propaganda war against the Franco-Russian coalition, making extensive use of intimidation, deception, and misinformation. Thus, in leaflets scattered from the German Zeppelins on the Eastern Front in 1915, it was stated that Anglo-French forces in the West were defeated, and the same fate awaited Russian forces and that to avoid "unnecessary bloodshed", Russian soldiers were offered a chance to capitulate[14].

---

[10] O. Dika, *Information warfare*…, op. cit.

[11] M.O. Kondratiuk, *The information war and the role of mass media in the international conflicts*, "Visnyk KNEU" 2013, Iss. 41, p. 33.

[12] H. Ibraieva, *Regional conflicts and the mass media*, http://psyfactor.org/lib/infowar3.htm, [accessed: 20.10.2019].

[13] M.O. Kondratiuk, *The information war*…, op. cit., p. 33.

[14] S. Neklyayev, *The mass media as the subject of the informational-psychological security*, "Media anthology" 2003, pp. 25–27.

World War I was the first war during which this means of demoralizing the enemy forces and population were actively used. For the first time, special units for propaganda appeared, and the technique of the propagation of printed agitation began to be created; the key elements of the "War of Words" were formed.

The concept of an "information war" combines two types of information warfare – information-technical and information-psychological.

N. Gurina, in "Information confrontation – one of the main directions of the policy of modern international relations", analyzes the methods of information war that were used during international conflicts in the context of national information security:

1. The events in the Persian Gulf in January 1991 and Yugoslavia in 1999, as well as the first and second Chechen wars in Russia, have changed the perception of the wars of the modern information society.
2. The Gulf War may be defined as the first full-scale operation of a new stage in the functioning of the military in a global information space. According to Z. Bzezynskiy, this conflict demonstrated the offensive aspect of the Pax Americana, which made it clear that the world would have to accept a "soft" American hegemony.
3. During the US military actions, the degree of openness was determined not by stable principles but by the current situation through "soft military censorship".
4. "Desert Storm" is no exception – the US military, using soft censorship, effectively removed messages that justified the opposite party from the information sphere. In addition, "Desert Storm" became the first live television-broadcasted war.
5. In turn, the Russian military was able to establish effective information support only in the second Chechen war.
6. During the aggression against Yugoslavia, information operations provided the necessary result – facilitating the actual capitulation of the Serbian armed forces.
7. The US seriously prepared for today's information confrontation. This is evidenced by the fact that full-scale work has been carried out in US military circles in this area. It began on December 21, 1992, when the US Department of Defense's T 3600.1 directive appeared. In the directive of the Chiefs of Staff Committee No. 30 of 1993 and in the US Army FM 100-6 Charter ("Information Operations") (1995), basic principles of information warfare were already given[15].

The US Doctrine of Information Operations identifies four main categories for the use of information against human intellect:

- against the will of the nation;
- against the enemy's military commanders;

[15] N. Gurina, *Information confrontation*..., op. cit.

– against enemy forces;
– against national culture[16].

In the context of the information security of the nation, media can play not only a negative role, forming an aggressive attitude towards the adversary in a conflict, but it can also use certain methods that can eliminate conflict and help resolve it without material or human loss[17].

O. Porfimovich claims that journalists can be peacemakers during a conflict. The media should find common values between the opposing parties and cover the events objectively by calling on the assistance of independent experts. The media should study the process carefully and cover the events, focusing on hope for the better[18].

Andrew Pudefatt, in Article XIX, believes that journalists are primarily obliged to inform the public impartially since their rapprochement with one of the parts of the conflict, even with its victims, may lead to doubts about the effectiveness and balance of their work[19].

However, just after the immediate conflict regulation in a society that does not yet have basic civilian institutions, liberal media without a clear nation-wide position is unlikely to be effective. It can only increase the division of a fragile society. According to Pudefatt, immediately after the conflict is settled, there may be a need to transform the existing national media into a national service created to provide citizens with balanced coverage of events.

UNESCO gives particular attention to independent media to preserve information security. Pudefatt, in the United Nations Educational, Scientific and Cultural Media, Conflict Prevention and Post-Conflict Recovery materials, emphasizes that the media provide a safe field for non-destructive conflict. That is why independent media are seen as an important element in shaping a democratic society. The main functions of the independent media are to provide information and monitor government actions.

> In societies that have overcome this or that crisis, independent media can provide substantial assistance in transforming a devastating conflict into a peaceful debate and enhancing the information security of the nation. The media can analyze the interests that hide behind each party's position in the conflict. This can help start a conflict regulation, find common interests, or at least provide the information needed to resolve the conflict. By empowering minorities or victims to voice their

[16] S.I. Hrynyayev, *The United States is deploying an information security system. In Russia, things do not go further than just talk*, http://www.4.narod.ru/warfare/grinyaev/page014.htm, [accessed: 20.10.2019].

[17] M.O. Kondratiuk, *The information war*…, op. cit., p. 33.

[18] O.L. Porfimovych, *Educational-methodical complex in the discipline "Conflictology" for students of specialty "Journalism"*, PE Tsymbalenko Ye. S. 2008, p. 48

[19] G. Slyadnyeva, *Legal regulation of access of state bodies to commercial confidentiality*, "Entrepreneurship, Economy and Law" 2005, No. 10, pp. 55–58.

position, the media can help be heard to those who are weak and depressed in the conflict[20].

According to US military experts, the main issue is shifting the emphasis in armed confrontation from its traditional forms of conduct (fire, strike, and maneuver) to the information-intellectual and information-technical spheres, where training is taking place and where military and political decisions are being adopted and implemented. Even a future war can be triggered by an information field that will cover the totality of tasks in the political, economic, technical, and military spheres[21].

The information war can be conducted both in wartime and peacetime, both at the national level (diplomatic, economic, informational, special, and other forces) and the military level (forces and other means of struggle with combat direction systems).

Several official documents, such as a report from the US Department of Defense "Report of the quadrennial Defense Review", the conceptual document of the US Joint Chiefs of Staff "Joint Vision 2010", and the report of the National Defense Commission "Transforming Defense National Security in the 21st Century, Report of the National Defense Panel", note: "We have recognized that the world continues to change rapidly. We are unable to fully understand or predict the problems that may occur in the world beyond the time limits of traditional scheduling. Our strategy accepts such uncertainties and prepares the armed forces to cope with them". "The acceleration of the speed of change makes future conditions more unpredictable and less stable, placing a wide range of demands on our forces". "The problems of the 21st century will be quantitatively and qualitatively different from those that characterized the Cold War, which will require radical changes in national security institutions, military strategy and approaches to defense issues by 2020"[22].

Major documents of the US Uniformed Services say that information influence is diverse and varies depending on the tasks and environment. The following directions of information influence are possible:

- surveillance and reporting activity (identification of military, economic, political, and cultural potential);
- counteracting any kind of enemy adversarial (OPSEC);
- distortion, neutralization, destruction, or, on the contrary, protection of information (CNA, CND);
- computer playback of a real or virtual environment and visualization of the battlefield;
- information-psychological (PSYOP) or physical influence on personnel, objectives, military equipment, weapons, and communication lines;

---

[20] O.L. Porfimovych, *Educational-methodical complex*..., op. cit., p. 49.

[21] M.O. Kondratiuk, *The information war*..., op. cit., p. 29.

[22] J.S. Nye, W. Owens Jr, *America's Informational edgel Strategy and force planning*, http://ics.leeds.ac.uk/papers/vp01.cfm?outfit=pmt&requesttimeout=500&folder=49&paper=155, [accessed: 20.10.2019].

- concentration on demonstrative actions, deception, and disorientation (military deception);
- radio suppression of telecommunication facilities, computer telecommunication networks, radio broadcasting equipment, etc.;
- reducing the visibility of objectives, military equipment, and weapons;
- protection of personnel, objectives, military equipment, weapons, and various radio-electronic means from the influence of electromagnetic or other energy;
- removal of self-guided weapons from the most important targets, etc.[23]

The basis of such influence lies first in psychological and ideological factors, as well as computer technology. This should not be reduced to classic special propaganda – the notion of "information influence" has a much broader meaning.

The documents also say that, at the national level, the main tasks of the information war are:

- US national security protection;
- getting the information that is necessary for making the military-political decisions.

Depending on the theater of war, the operational environment, and the tasks to be accomplished, any component of these forces can play a decisive role. A new problem that has arisen is the integration of information wars into the overall national security strategy. US experts stress the need to develop a unified concept of national information security, which includes both military and financial, trade, psychological, legal, and other aspects of defense and offense. At the same time, the main strategic goal of offensive information actions moves from active influence on automatic systems and weapons to the individual, that is, to the decision-maker. According to experts, such actions may be most effective in peacetime and in the early stages of the conflict, which is in agreement with the main goals of the US national security policy[24].

Based on the forecast of strategic conditions until 2020, US military experts have identified and stated in official documents, several major trends in world development that pose potential problems for the US. Of course, conclusions based on the forecast of development trends can be relatively accurate only in the near future (from one to three years). After that, their accuracy is lost. Some trends (such as demographics) can be tracked with a high degree of accuracy. Others (geopolitical types) are less predictable, as they change more quickly under the influence of different events.

US military analysts conclude that although nations remain the dominant units of the international system, they will increasingly be influenced by the power of multinational corporations and international organizations. The development of technology, geopolitical transformation, demographic pressure, and the strengthening

[23] A. Levakov, *The USA is preparing to protect the information systems*, http://www.4.narod.ru/index.html, [accessed: 20.10.2019].

[24] J.S. Nye, W. Owens Jr, *America's Informational*…, op. cit.

of economic and social trends can radically change the realities of today. The possible scenarios are far-reaching and difficult (or impossible) to predict. Therefore, a central problem for the defense structure is development in a direction that will allow it to respond effectively to any variant of events. This determines the need for constant adaptation of forces to existing trends[25].

In formulating the terms "information war" and "information security", China's military analysts interpret them in a narrow and broad sense. In a narrow sense, information warfare is a field information war, that is, combat operations in the field of military management. These include the active use of reconnaissance, misleading and masking measures, psychological operations, the consistent defeat of other information systems, combat and communications systems, and the protection of its own systems.

Chinese military experts are paying close attention to foreign developments in the field of information warfare. Like Western military experts, they believe that information warfare is not a literal war on the battlefield, prepared for with training and maneuvers. Recent armed conflicts have prompted experts to highlight some of the traits inherent in the information war.

International information security should be considered as a policy that promotes effective guarantees of peace for both the individual country and the world community. Among the noteworthy theoretical views on international security, it is worth mentioning the French theorist Raymond Aron, who believed that security in the world of independent states could be based either on the weakness of rivals (their full or partial disarmament) or the strength of the nation[26].

Due to the global nature of the information security problem, developed countries have started implementing long-term national programs aimed at ensuring the protection of critical information structures, and, since 1996, the problem of international information security has been raised to the political and international-legal level:

- the concept of international information security was discussed at an international conference on the problems of becoming an information society and global civilization (Republic of South Africa, 1996);
- the joint communiqué of the US-Russian Summit highlighted the threat of information weapons and acknowledged the presence of a military component in the global informatization process;
- resolution 53/70 of December 4, 1998, was adopted by consensus at the 53rd session of the UN General Assembly. It states that the international community recognizes the problem of information security as a multidimensional strategic direction for the interaction of countries in the world, and invited member states to consider a specific typology of information threats, identify criteria for the problem, including the development of international security principles

[25] A. Levakov, *The USA is preparing*…, op. cit.

[26] A. Raymond, *Memoirs: 50 Years of Thinking about Politics*, Ladomyr 2002, p. 873.

for global information systems, and submit proposals for a comprehensive report by the UN Secretary-General to create an international mechanism for the idea of using information weapons and sparking information wars[27].

During the discussions and consideration of applied aspects of the international information security of media organizations, the specifics, essential characteristics, and typology of information threats were defined, and the terminology and content of basic concepts in the new sphere of international cooperation were agreed.

In international circles, information security is defined as the interaction of the members of international relations with the operations of maintaining a sustainable peace based on protecting the international infosphere, global infrastructure, and public consciousness of the world community from real and potential information threats.

The infosphere is an international information space covering information flows, information resources, and all spheres of life in civilization. The infosphere can also be defined as cyberspace, which includes the media[28].

International information operations are characterized as a form of inter-state confrontation, which is realized using information influence on the systems of management of other states, as well as on the political power and society in general, on infrastructure, and on mass media to achieve the advantage and ultimate purpose of the information operation and the simultaneous protection of the national infosphere from similar actions.

Depending on their use, information security practices take on several aspects. In the most general form, information security is a state of protection of a society's information environment, which ensures its formation, use, and development for the benefit of citizens, organizations, and the nation[29].

The recognition of the problem of information security at the international level is conditioned by such factors of globalization of communication as, for example, the fact that in most industrialized countries, research and development of new information weapons are carried out in such a way as to allows direct control over the information resources of a potential adversary and, if necessary, directly influence it. According to US think tanks, the development of such weapons is observed in 120 countries. For comparison, developments in the field of nuclear weapons are conducted in 20 countries. In some countries, the development of means of information warfare with a possible adversary is fully completed, both in conditions of military conflicts of different intensities and in peacetime at strategic, operational, and tactical levels, and in the field, to protect the national infosphere from aggression and unauthorized intervention. In developed countries, the concept of information

[27] *International information security: Modern challenges and threats*, Free Press Centre 2006, pp. 13–14.

[28] S.I. Hrynyayev, *The experts of "RAND" corporation about the information strategy*, http://attend.to/commi, [accessed: 20.10.2019].

[29] O.K. Yudin, V.M. Bogush, *Information security of the nation*…, op. cit., p. 576.

warfare is part of the military doctrine, which requires special training of personnel and individual units for conducting information operations. The practice of international, regional, and ethnic conflicts revealed the uniqueness of using information weapons to influence the international community and fight for geopolitical interests[30].

Today, many countries have long been engaged in the policy of protecting information flows and systems – not only as sources of national secrets but also as sources of economic profit. France, for example, was successful in creating its own segment of the Internet in French. It has taken control over the lucrative market of computer hardware, software, and information streams across the French-speaking world. One of the best known, however, is the Chinese experience. China has achieved significant economic growth by reorienting information flows and capital accumulation in the information field[31].

It was observed that global information warfare strategies are at the heart of the analytical developments of research institutions in different countries, aiming to provide information leadership in the field of international security. According to the research, analysts distinguish the following models of global information security systems:

Model A is creating an absolute system of protection for the information-leader country against any kind of offensive information weapon, which causes objective advantages in a potential information war, forcing other countries to seek an alliance in military-information actions with a country-leader. In this case, a system of tight control over the enemy's information weapons may be used based on potential international information security documents.

This development is considered in the famous study "America's Information edge strategy and force planning" by J. Nye and W. Owens (1996), which affirms the dominant role of the US in the information revolution, that is, in the use of powerful communications and information technologies (satellite surveillance, live broadcasting, high-speed computers, unique capabilities in integrating complex information systems), policies to contain and neutralize traditional military threats, and new weapons.

Model B is creating a significant advantage of a potential initiator of information warfare in offensive weapons, degrading opposition protection systems by information impacts, and coordinating actions with allied states using certain information weapons to identify sources and types of information threats.

The practical implementation of the model is seen in the Allied Forces (1999) information operation conducted by the US and NATO member states against the Federal Republic of Yugoslavia. Experts emphasize the formation of an unprecedented scale of information flow management systems for conducting military operations (the ability to provide intelligence directly to each of the combatants), mass

[30] *International information security*…, op. cit., p. 916.

[31] O. Dika, *Information warfare*…, op. cit.

propaganda campaigns with a wide range of information techniques (from PR technologies to form a favorable world community opinion, sample informing with the intended effect of perceiving content to the widespread discrediting of adversary policies, as well as outright misinformation of the world community), targeted information and psychological influence, and the powerful computer and Internet use in confrontation to modify the national information space and control over the infrastructure of Yugoslavia. New strategies for information operations demonstrated by the US and NATO show the power of information weapons in developed countries and the need for an international solution to the information security problem[32].

Model C includes the presence of several information-leading countries and the potential confrontation between them, determining the factor of the deterrence against the expansion of information threats, and ensuring the possible dominancy of one of the countries in the field of international information security with the potential to significantly influence the global infosphere and the prevailing right to solve the problems of the global order.

CIA research in the 1990s for further extension to 2020 identified Russia and China as the only two countries constituting major sources of cyberspace threats to the US. The new military doctrine of the US Armed Forces (Force XXI Concept, 1996), which offered two components of a theater of war – traditional space and cyberspace – considers the information infrastructure and the human psychological network as the main objects of influence[33].

At the present stage, US experts say that strategies of various types of information operations against the country are planned and implemented by more than 20 countries, and the states confronting the US include information war in their military doctrines. Therefore, as a deterrent against expansion in the international information space, the Force XXI strategy is a tool for the US's informational superiority in a global confrontation.

Model D claims that all parties to the conflict use transparency of information to form situational alliances, achieve the benefits of local decisions that can block technological leadership, use infrastructure capabilities in individual territories to organize internal conflict between opposition forces (political, separatist, inter-conflict), and conduct international counterterrorism information operations.

In the context of the international anti-terrorist Operation Vengeance (Afghanistan, 2001), the purpose of the specialized US centers responsible for information operations was to plan psychological campaigns, respond to changes, maintain information resources, and secure the military and civilians. "The US intended to neutralize and destroy the entire terrorist network that threatens America and the rest

[32] S.I. Hrynyayev, *Features of the information war during the NATO aggression against Yugoslavia (based on open press materials)*, http://www.4.narod.ru/warfare/grinyaev/page-008.htm, [accessed: 20.10.2019].

[33] Idem, *Information war*…, op. cit.

of the civilized world", US Secretary of State K. Powell said at a press conference for the international mass media.

> The purpose of Operation Vengeance was not only to counterterrorism, but also to convince certain regimes that support terrorism policies that such a strategy does not meet their own interests. The US was pleased with the response from the global community and political leaders of most countries to global counterterrorism proposals[34].

For example, for the first time in history, the Northern Alliance has applied Article 5 of the NATO Treaty, which seeks to ensure the overall protection of member countries against external threats. The EU Member States and GUAM Member States reaffirmed their support for US action in Operation Vengeance and consolidated the international community's efforts to counter international terrorism in a joint statement and memorandum of action. Russia's political leader V. Putin has proposed to develop a new system of global security, taking into account that terrorism and its varieties of media and cyberterrorism have become a global threat to international peace in the twenty-first century.

"USA Today" presents a model of the information war against the Taliban, which includes conducting a psychological operation in Afghanistan's information space while simultaneously blocking national radio stations, distributing propaganda material with the extracts from the Quran to counter calls for jihad, and formulating the feeling of inescapable victory over the counterterrorist alliance during Operation Vengeance.

Model E is a confrontation between the world community and international organized crime, which can control the flow of political, economic, social, and, ultimately, civilizational processes. The possibility of such a model is envisaged in the study of the National Intelligence Council of the US "Mapping the Global Future" for 2020 in the version of "Cycle of Fear", which is the most pessimistic scenario for the future world community.

Considering the substantial capacity of information weapons to integrate with other traditional and technologically new types of military means, the potential consequences of the uncontrolled, multilayered use of them may be catastrophic for humanity. Therefore, only wide-ranging multidimensional cooperation can guarantee worldwide solutions to the new, complex problems of the information age and ensure real international information security[35].

Conclusions

The problem of information security is a significant component of the common concerns of national, regional, and global information relations policies, the manifestation of new global challenges, and deep processes of the globalization of communications.

---

[34] N. Gurina, *Information confrontation*..., op. cit.

[35] *International information security*..., op. cit.

The experience of the information-developed countries shows that there are economic advantages in the modern world based on the progressive expansion of information, and countries that have advanced the most in the direction of information civilization will prevail in the world economic system and in international competition with technologically backward countries and regions. Today, the concept of total war in the traditional sense, which is the basis for strategic guidelines in many countries, is outdated. There is a strong reason to believe that the world is entering a period of a new generation of wars, aimed not at the immediate destruction of the enemy but at achieving political and economic goals without fighting between large armies.

Therefore, it should be concluded that in modern conditions, information security becomes an organic element of national security since information is transformed into a resource not only of national strategic importance but also of global importance. Accordingly, the development of concepts, strategies, purpose-oriented programs and action plans for Ukraine's national security should take into account changes in the space of threats and challenges caused by the widening influence of the information factor in the context of globalization.

The phenomenon of information security is due to the strategic orientation of information weapons against the critical structures of life and the functioning of the international community, and the recognition of information weapons as a new type of global weapon of mass destruction, with potentially catastrophic consequences (some researchers call information weaponry an informational apocalypse). This phenomenon is also due to the necessity of creating an international tool for the counteraction and prevention of global information wars within the framework of the UN's political competencies, regional organizations on security and defense, and policy decisions at the national level.

Therefore, information security is a significant component of the common problems of national, regional, and global information relations policy and the manifestation of new global challenges and deep processes of the globalization of communications.

It was noted that the media could create negative feelings and tensions among people, but it can also help opponents find common ground during and after conflict settlement. In general, in the current context, the media is of great importance in times of conflict. The facts covered by the media and the emphasis on certain phenomena or aspects of confrontation shape the audience's opinion about the conflict, stimulating the desired reaction. The media provides an opportunity to turn a small conflict into a major confrontation or, conversely, to eliminate a serious problem quickly. The course of the conflict itself depends on the bias and involvement of the media and its attitude towards the event.

References

Badrak V., *Factors of effectiveness of influence of mass media on electorate*, extended abstract of Doctor's thesis, KNU 2000.

Blumer G., *Collective behaviour* [in:] *American Sociological Thought. Texts*, D. Vodotynskogo (eds.), Izd-vo MGU 1994.

Dika O., *Information warfare. Modern tendencies of web communication*, http://webstyletalk.net/node/97, [accessed: 20.10.2019].

Gurina N., *Information confrontation as one of the main directions of the policy of modern international intercourse*, http://www.experts.in.ua/baza/analitic/index.php, [accessed: 20.10.2019].

Hrynyayev S.I., *Features of the information war during the NATO aggression against Yugoslavia (based on open press materials)*, http://www.4.narod.ru/warfare/grinyaev/page008.htm, [accessed: 20.10.2019].

Hrynyayev S.I., *Information war: History, today and outlook*, http://www.4.narod.ru/warfare/grinyaev/page009.htm, [accessed: 20.10.2019].

Hrynyayev S.I., *The experts of "RAND" corporation about the information strategy*, http://attend.to/commi, [accessed: 20.10.2019].

Hrynyayev S.I., *The United States is deploying an information security system. In Russia, things do not go further than just talk*, http://www.4.narod.ru/warfare/grinyaev/page014.htm, [accessed: 20.10.2019].

Ibraieva H., *Regional conflicts and the mass media*, http://psyfactor.org/lib/infowar3.htm, [accessed: 20.10.2019].

International information security: Modern challenges and threats, Free Press Centre 2006.

Kondratiuk M.O., *The information war and the role of mass media in the international conflicts*, "Visnyk KNEU" 2013, Iss. 41.

Levakov A., *The USA is preparing to protect the information systems*, http://www.4.narod.ru/index.html, [accessed: 20.10.2019].

Lyzanchuk V., *The phenomenon of the immortality of the war*, "Scientific Notes of the Academy of Sciences of Ukraine" 2004, Iss. 6.

Neklyayev S., *The mass media as the subject of the informational-psychological security*, "Media anthology" 2003.

Nye J.S., Owens W. Jr, *America's Informational edgel Strategy and force planning*, http://ics.leeds.ac.uk/papers/vp01.cfm?outfit=pmt&requesttimeout=500&folder=49&paper=155, [accessed: 20.10.2019].

Porfimovych O.L., *Educational-methodical complex in the discipline "Conflictology" for students of specialty "Journalism"*, PE Tsymbalenko Ye. S. 2008.

Raymond A., *Memoirs: 50 Years of Thinking about Politics*, Ladomyr 2002.

Slyadnyeva G., *Legal regulation of access of state bodies to commercial confidentiality*, "Entrepreneurship, Economy and Law" 2005, No. 10.

Yudin O.K., Bogush V.M., *Information security of the nation*, MK-Press 2005.

The international experience of the information security of the nation

Abstract

The article analyzes the political aspects of national information security in the context of global information influence. It is noted that, in today's world, information security plays an important role in the context of the ongoing globalization of the information society. The information security of the nation needs to achieve a state of security, that is, to create and maintain appropriate engineering and technical facilities and information organization that meet the real and potential threats, as well as the demographic and economic situation of the country. It is established that information security is relevant to one degree or another for all states and is a significant component of the common problems of national, regional, and global policy in the field of information relations. The power of engineering, hardware, and software methods of national security in different countries varies and depends on a set of conditions associated with the potential internal and external threats and the nature of relations with neighboring states and geopolitical centers.

Słowa kluczowe: bezpieczeństwo informacyjne, wojny informacyjne, geopolityka, środki masowego przekazu, wpływ mediów, narody

Key words: informational security, information wars, geopolitics, mass media, media influence, nations

Iryna Patlashynska

Graduated with degrees in international law at the Institute of International Relations of Taras Shevchenko National University of Kyiv and political processes and institutions at the Lesia Ukrainka Eastern European National University. She is also a Spanish translator. In 2009–2011, she was an employee in the Department of International Relations of Lesia Ukrainka Eastern European National University. Since 2011, she has been a lecturer at the Department of International Communications and Analysis of the Faculty of International Relations. Her research interests include various branches of international public law, information security, and international organizations. E-mail: eleonora.777@hotmail.com