International experience of legislation ensuring of public information security

Yurii Khatniuk, Lviv State University of Internal Affairs

Taras Tymchyshyn, Lviv State University of Internal Affairs

Oleg Batiuk, National University Odessa Law Academy

Oleksandra Hrynkiv, State Border Guard Service of Ukraine

Nelia Otchak, Lviv State University of Internal Affairs

Abstract

Nowadays, the neutral countries are fully aware of the immediate dependence of their well-being on the information sphere, and therefore, the issue of information security has naturally taken a prominent place in the security strategies of the respective countries. At the same time, the policy of information security for non-aligned countries is proactive and is based on the principles of information security risk management, first of all, on the cybersecurity. The problems of ensuring the information security of the individual, the society, the state, their protection against various kinds of threats, both external and internal, now occupy one of the main positions in the priorities of state policy and national security strategies of the countries of Central Europe, which, in their turn, focus on EU and NATO standards in the case of this problem. It has been found that information and communication technologies at the current stage are under increasing military influence. The forecast presupposes that further refines of the methods of conducting information and psychological warfare and expanding the spheres of application of relevant technologies, which at the global level can significantly affect the strategic balance of forces, cause changes in approaches to its assessment based on the correlation of geopolitical, economic and military factors. The complexity of the incident's source identification in the information space together with the inconsistency in the problem of what measures are acceptable in response to this incident increases the likelihood of a conflict and damage to a particular area of the country or countries.

Keywords

Information Security, Legal Regulation, Strategy, Policy, Cyber Attack.

Introduction

In recent years, the paradigm of information security in our country has changed significantly. First of all, the very nature and, accordingly, the strategic dimension of the concept of ensuring the information security of the country have been transformed.

At the same time, the information security of the country does not appear as something virtual, an abstract object of scientific knowledge, but as a completely real subject within which fierce fights occur and there are obvious threats with obvious consequences. We can confidently say that the own model of information security is created in many countries of the world, the one which is based solely on their own experience of both its legal and operational support.

The European countries, which can be conditionally united under the name of non-aligned ones, are among the most developed countries on the continent, in particular in issue of the rate of development of the information society, as well as the awareness of the need to countering cybersecurity threats, the protection of information and critical information infrastructure and the information-psychological security of citizens and ensuring the information security in general as a component of national security.

The purpose of the research is the formation of theoretical and methodological bases of legal support of information security of the country by development of theoretical bases of information law and formation of proposals for improvement of information legislation.

The outlined research purpose is associated with a solving a significant theoretical and practical problem-the development of conceptual legal foundations for ensuring information security of the country and forming practical recommendations for improving mechanisms of its realization.

The hypothesis of the research is based on the assumption that ensuring the information security of a country will be effective on condition of its proper legal support and scientific justification of the relevant recommendations for improving information legislation.

Literature Review

It is quite clear, that even adequate to social reality both current and future scientific considerations on the issue of information security, will be rather dubious without the basis on the classical heritage (Dhillon et al., 2017; Dean & McDermott, 2017).

At the same time, it is equally obvious that the creativity of the most prominent representatives of world philosophical thought, despite its undeniable value and inevitable relevance, does not exhaust all aspects of the philosophical understanding of the problem of information security (Lee et al., 2017).

And, by the way, their views are demonstrative both in the aspects of their opposites and their unity, which can become a promising aspect of understanding the essence of information security, around which the future system of information security will be built, both at national and global levels (Cherdantseva & Hilton, 2013; Govender, 2015).

At least the modern methodological approaches to the socio-philosophical analysis of the phenomenon of information security should incorporate as many positive elements of the analyzed historical heritage as possible.

A retrospective analysis of this problem is needed to select a promising methodology for the research on information security issues (Barkatullah, 2018).

Nowadays, the terms of information war, information confrontation, informational influence, information weapons, etc. have become known in the global media space, in journalistic and scientific works, as well as in the political and government documents of many countries. The information and communication technologies (ICT) play a key role in world politics, economics and security systems (Priisalu & Ottis, 2017).

The information sabotage in the cyberspace today involves both organized groups and individuals. An increasingly important component of countries military capabilities is IT weapon as the addition to their own military arsenal (Zhang & Liu, 2017). In this case, the information wars between countries can be no less devastating and violent than traditional ones.

The accumulated theoretical and practical experience on the formation of an information security system demonstrates the considerable contradictions in the legal regulation of relations in the national information space. Having analyzed the source base and comprehending the realities of creating a system of information security, theoretical and practical problems have been identified, starting from the lack of sufficient theoretical bases of information security to the lack of systematic and insufficient effectiveness of the relevant practices.

Methodology

Philosophical (dialectical, metaphysical), general theoretical, (epistemological, structural-functional), special (comparatively legal, inductive) and inter-branch methods of scientific cognition (historical, analytical) have been used as the methodological basis of the study.

The formal and legal method made it possible to examine the competence of the subjects of information security of the country, and it was also used in interpreting the rules of law to clarify their essence, content and the will of the legislator expressed in them. The structural- functional analysis made it possible to determine the conformity of the normative-legal acts with which the modern system of legal provision of information security of the country is associated, to the real social relations in this sphere and to international standards.

Findings and Discussion

With the end of the Cold War, the bipolar world became much more complicated, so the concept of non-accession, non-participation in military-political alliances, etc., lost its self-worth. In particular, the notion of neutrality that is associated with non-participation in wars has been deprived of its direct meaning. That’s why such status of a number of European countries remains largely a tribute to historical traditions. Today, such countries are indicated as post-neutral or non-aligned. Each of these countries has its own history of neutrality, but over the last 20 years, they have all encountered the problem of feasibility of preservation of the neutral status and the need to impose some forms of restrictions on it. The same trend remains actual nowadays, due to the situation that the international processes and the substantive content of new threats, including regional conflicts and international terrorism, the proliferation of weapons of mass destruction as well as cybercrimes, require concerted action and large-scale cooperation from the international community.

Switzerland, which is neither a NATO nor an EU member, holds a special place among the non-aligned countries.

Since 1992, the Federal Data Protection Act has been in force in Switzerland, it embodies pan-European principles for the protection of information, including so-called 'sensitive' information and, in particular, personal data (Carrapico & Barrinha, 2017).

In 2010, Federal Supreme Court of Switzerland provided additional guarantees of the personal data confidentiality, maintaining a local data protection officer and adopting an order according to which the collecting of the information about the IP-addresses of the file sharing users without their consent (inclusively in the context of copyright infringement) is illegal (Carrapico & Barrinha, 2017).

The prerequisites for reducing cyber risks are individual responsibility and national cooperation between the private sector and the authorities, as well as the cooperation of the countries one with the other. The state should intervene in cybersecurity processes only when the public interest is threatened or if it complies with the principle of the subsidiarity.

Cyber risk management should be seen as an element of business processes, of the production or the management processes that involve all the subjects, starting from the administrative and technical levels to the senior management. An effective approach for cyber risk management, that is based on the principle of sharing the responsibilities between government, the private sector and the people, implies that each organizational unit (political, economic or social) is responsible for knowing about cyber aspects and for eliminating information risks, associated with the specific processes, or minimize them if possible.

In early 2018, Switzerland began the development of the information security law. It was accepted that the illegal use of information and interference with the information systems could seriously affect the essential interests of the country and the rights of its citizens. Based on universally accepted international standards, the law on the information security should provide a single formal legal basis for the control and the implementation of the information security within the competence of the Federal Council of Switzerland.

First of all, the law concerns the federal government authorities: the Parliament, the federal courts, the prosecutors' office, the National bank, etc. The private individuals and the businesses are the subjects to the law if they carry out the 'sensitive' information activity on behalf of the federal authorities. The Federal Council also seeks the opportunities for deepen cooperation with the cantons, which should be represented in the appropriate coordinating body and should participate in the processes of the standardization of the appropriate measures. Inter alia, the law regulates the risk management issues, classifies the information and sets the security principles on the use of IT resources. The information security law is planned to have the priority over the legislation on the freedom of the information (Anwar et al., 2017).

We consider it appropriate to continue the research with studing the experience of providing the information security of the European countries which are non-NATO but EU members, such as Austria, Finland and Ireland. First of all, we want to mention that the EU membership imposes the obligations on these countries to comply with the organization's standards for the information society development and the information security. Thus, in 1991, the European Information Technology Security Evaluation Criteria was developed (Giancaspro, M. (2017)), which in particular defined the tasks of ensuring the information security, namely:

1. The protection of the information resources from the unauthorized access in the issue of confidentiality;

2. The esurience of the integrity of information resources by protecting them from the unauthorized modification or the destruction;

3. The esurience of system performance by countering to the threats of the denial in the service.

In 1996, the standards of European information security were realized in "*Common Criteria for Information Technology (IT) Security Evaluation*" (Sun et al., 2018).

In Austria, Finland and Ireland, as in other EU countries, the considerable attention is paid to the cybersecurity issues and is stated in the European Commission's Resolution "*Towards a general policy on the fight against cyber crime*", where the latter is defined as criminal offenses committed using the electronic communications networks and information systems or against such networks and systems, namely:

1. The traditional forms of crime (the fraud and the forgery in the electronic communications networks and in the information systems);

2. The publication of illegal content in the electronic media;

3. The specific crimes in the electronic networks (the attacks on information systems, the hacking, etc.).

4. The main challenges for the information security of these countries, as well as of the EU as a whole, are:

5. The uncoordinated domestic approaches to the security of the information infrastructure, which reduces the effectiveness of national measures;

6. The lack of European-level partnerships between the public and private sectors;

7. The limited opportunities for early warning and the response to security incidents, due to the uneven development of monitoring and incident reporting systems in Member-States, the underdeveloped international ooperation and the exchange of the information on these issues;

8. The lack of international consensus on the priorities in the implementing of the policy of the protection of the critical information infrastructure.

Ireland's National Cybersecurity Strategy for 2015-2017 has envisaged that the Government would make every effort to ensure the sustainable and safe operation of computer networks and related infrastructure by Irish citizens and businesses. The development and the dissemination of the information and communication technologies has contributed to a significant improvement of the quality of life, the emergence of the innovative services and the radical changes in the organization of the business. Therefore, the state, the critical infrastructure, the legal entities and the citizens depend on the reliable functioning of the information and communication technologies and the Internet. The disruption of these systems, whatever their source, creates a direct threat to the functioning of the state mechanism and the economy, it can significantly affect the daily lives of millions of citizens. Therefore, any threat to cyberspace security requires a timely, reliable and consistent response, both on the national and on the international levels.

To this end, the Government of Ireland has outlined the following tasks for the relevant entities in the country:

1. To increase the resilience and reliability of critical information infrastructure in key sectors of the economy, especially in the public sector;

2. To continue the engagement with international partners to ensure that cyberspace remains open, secure, coherent and free, as well as capable of promoting the economic and social development;

3. To raise the awareness of the responsibility of the business and the individuals to ensure the security of their information networks, the infrastructure and the data, and to maintain such awareness by the means of the information, training and practice;

4. To provide a comprehensive and flexible regulatory framework for the governmental authorities to combat cybercrime that is relevant and proportionate to the needs of the protection of ‘sensitive’ or personal data;

5. To create the capacity for the government and the private sector to operate and manage cyber accidents.

Recommendations

The analysis of the mentioned international documents makes it possible to identify the priority areas of the information security in these countries:

1. The raising of the awareness of the users about possible threats when using communications networks;

2. The creation of a European system of warning and notification of new threats;

3. The providing of technological support;

4. The support for market-oriented standardization and certification;

5. The legal support, the priorities of which are the protection of personal data, the regulation of telecommunications services and the fight against cybercrime;

6. The strengthening of the information security at the state level by introducing effective and compatible means of ensuring information security and encouraging the use of electronic signatures by Member-States when providing public online services, etc.;

7. The development of the international cooperation on the information security.

Based on the above, we can identify the main areas of the international activity in the case of ensuring the international information security (IIS), namely:

1. The creation of the conditions at the national and at the global levels for the development, production and implementation the means of ensuring of the IIS;

2. The organization of effective the international ICT-cooperation;

3. The joint fight against cybercrime and the information terrorism;

4. The safeguarding of the ICT in the case of harmful effects and reducing the potential harm from attacks on the information systems;

5. The improvement of the personnel support and the organizational measures, the methods of training of the specialists and carrying out of the scientific researches in the field of the information security and cybersecurity;

6. The international activities aimed to prevent conflicts in the information space, as opposed to the approaches that entail legitimizing of them;

7. The protection of the information and its processing means for the successful implementation of the complex scenarios at all levels;

8. The comprehensive research on the use of the ICT in conflicts and the applicability of the international law to states' actions in the information space.

Accordingly, the following steps, which are aimed at the building of confidence and reducing the risk of misperception of the situation in the case of disorganization or disruptions related with the usage of the ICT, should include:

1. The continuation of the inter-state dialogue on the norms of the state use of the ICT for reducing the collective risks and protecting of critical national and international infrastructure.

2. The developing and implementing of the effective confidence-building measures, the enhancing of the global stability in the ICT field, including the exchange of views at state level on the implications of the public use of ICT and their use in conflicts.

3. The interstate exchange of the information on the national laws, the strategies, the technologies, the principles and the best practices for ensuring the information security.

4. The identification of the list of measures that will contribute to creation of the potential conditions for the information security in the countries with less developed ICT.

Conclusions

At the present stage, the information and communication technologies are under increasing military influence. On the basis of the realities, it is not difficult to predict the further improvement of the methods of conducting the information-psychological warfare and the expansion of the spheres of application of relevant technologies, which at the global level can significantly affect the strategic balance of forces and cause changes in the current criteria of its assessment based on the ratio of geopolitical, economical and military factors.

The complexity of identifying the sources of the incidents in the information space, the lack of consensus on the problem of what measures are appropriate, create the risk of inadequate threat assessment, and thus they increase the likelihood of the emergence of the conflict and damage to one or another sphere of state's activity. Against this background, the current threats to information security are the following:

1. The increasing likelihood of the application of the ICT in future conflicts taking into account the enhancing of ICT capabilities for military, intelligence and political purposes, which a number of countries is applying. At the same time, the varying level of ICT security capabilities currently under way in an interconnected world increases the vulnerability of public entities with less ICT potential;

2. The possibility of attacks on critical infrastructure and related information systems of states using ICT;

3. The possibility of using ICT with criminal intent to carry out terrorist attacks on ICT objects or the infrastructure related with them;

4. The likelihood of global threats to peace and security through the use of ICT for terrorist purposes to recruit supporters, secure terrorist attacks, train members of terrorist groups, etc.;

5. The significant heterogeneity of the malicious non-public entities (including criminal groups and terrorists), their motives, etc.

6. The rapid nature of the malicious attacks in the ICT field and the presence of a large number of malicious tools and methods that hackers use, besides the fact that the arsenal of attackers on ICT is constantly improving and becoming more effective;

7. The ability to use ICT for propaganda, disruption, exchange, collection, transmission of the information, including the introduction of malware to undermine trust to the certain state, non-governmental, commercial entities, individual programs, goods, services, etc.

At the international level, the concerns of public entities cause the attempts of controlling the global information space through ICT. At the same time, the issue of respect for human rights and the provision of fundamental freedoms in the information field is of particular importance. Meanwhile, the observance of these rights and freedoms should not contradict the two most important principles of the international law such as the non-interference in the internal affairs of states and the respect for national sovereignty.

We believe that the interstate agreements and the international information law will be aimed at demilitarizing of the international information space. It is necessary to refine and adapt the mechanisms of international law in the field of information and communication technologies, as well as to create new norms, because the arms race in the information space can lead to the destabilization of the international security by violation of existing disarmament agreements and the agreements in other spheres.

References

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior, 69*(1), 437-443.

Barkatullah, A.H. (2018). Does self-regulation provide legal protection and security to e-commerce consumers? *Electronic Commerce Research and Applications, 30*(1), 94-101.

Carrapico, H., & Barrinha, A. (2017). The EU as a coherent (cyber) security actor? *JCMS: Journal of Common Market Studies, 55*(6), 1254-1272.

Cherdantseva, Y., & Hilton, J. (2013). A reference model of information assurance & security. *International Conference on Availability, Reliability and Security, Regensburg.*

Dean, B., & McDermott, R. (2017). A research agenda to improve decision making in cyber security policy. *Penn State Journal of Law and International Affairs*, *5*(1), 1-29.

Dhillon, G., Syed, R., & S