

POLITICAL AND LEGAL FOUNDATIONS OF INFORMATION SECURITY IN THE MODERN WORLD

Shafag Ahmedova¹

Azer Shirinov²

Abstract: The analysis of the current political and legal foundations of information security and comparison of its different historical stages have proved that many factors directly affect this process. They include inter-state historical relations and the world order, the struggle of various countries and regions for resources, the development of information and communication technologies, as well as the self-awareness of people. The authors of the article have concluded that information security lays the basis for state security in general and increases its power. The level and nature of communication between countries and their blocs are determined by the ability to influence each other through a system of propaganda and communication routes, including goods, services, the education system, scientific studies and social networks. Cybercrime can be combatted not only through toughening political

and legal restrictions but also through forming a global humanitarian approach to human values, which is ensured by the education system, the exchange of universal cultural values and the formation of new human qualities. The political and legal foundations of modern information security are as follows: historical relations between various states and regions; the current world order as the leading factor in forming the concept of information security; the power of each state and its role in the international security system as a political actor; the nature and development of information society in each region of the world; a set of international laws and treaties regarding the use of information, its preservation and disposition; the legal framework of each state; general trends in the formation of the global information space and its features associated with information and communication

Institute of Philosophy, National Academy of Sciences of Azerbaijan, Baku, Azerbaijan¹
Baku State University, Baku, Azerbaijan²



technologies. Information can work to the benefit only if different countries and regions cooperate since their interdependence grows each year, including in the sphere of information support. To obtain these results, system analysis of the legal framework of economic security, both in individual countries and internationally, as well as an abstract logical analysis of the practice of making political decisions to ensure information security were used. The rules and guidelines of information security, described in the scientific literature, as well as applied in practice in individual countries, have been studied.

Keywords: global political system, information as a political category, social-political regime, legal aspect of information security, information and communication technologies and cyber terrorism, information security

Introduction

The current world order provides for a balance between states based on their power and historical position in some region (Schweller, 2016). However, this balance cannot be stable for a long period. Any changes in

476

the internal political development and current state of certain regions form new priorities and interests of countries and international political blocs. As a result, a new political situation emerges that can be acute and conflict-ridden. Political theorists emphasize either material powers or ideological factors (Paul et al., 2004). We should note that the concept of soft power gains more popularity among politicians and theorists since it contributes to achieving equilibrium in the world order (Schweller & Pu, 2011). Despite the priorities associated with material resources, an increasingly important role is played by a comprehensive assessment of specific world development where all parties are interconnected. When analyzing the aggregate factors determining the interconnection and development of countries over the globe, special attention should be paid to information support that has recently been the subject matter of many studies both within the framework of general political processes and information security (Cybersecurity Trends, 2020).

The expansion of information space through the development of information and communication technologies has led to revolutionary



changes in many areas of social life. Due to these technologies, the availability of information increases attempts to appropriate it, especially the data directly related to political security. Thus, the legal basis for information protection both within some state and outside its borders began to develop at full speed (Kornblum, 1985). In general, there is a greater need for preserving and transferring information from one subject to another, including at the state level. During the early formation of industrial capital, invention secrets were easily kept and passed from one generation to another. In the conditions of scientific and technological progress, it is practically impossible to keep any information secrets. Since the second half of the 20th century, many countries have imposed special rules and restrictions in the form of laws, treaties and other security measures for the needs of information security.

The methods of information transfer have become much more sophisticated: "increasing sophistication with respect to the storage, retrieval and transmission of information; [...] future, electronic equipment, including computers, will become much more sophisticated" (Wall, 1972). In this

477

regard, countries use common global networks (Internet) and restricted means of transmitting information (encryption, special messengers, secret mail, etc.).

The ability to influence public consciousness through the targeted supply of information has become an important aspect of information processes. The concepts of "information war", "information bomb", "information defeat", etc. have become widespread (Redhead & Virilio, 2004). In addition, strategic programs of "network-centric warfare" are developed (Persson, 2017) which purposefully use information, network and propaganda flows to mold people's consciousness, motivation and interests. A. Dugin emphasizes that "a decisive factor might be the information environment where it is happening, i.e. the position of the parties involved in a potential conflict. Therefore, priority should be given to environment preparation both at the local and global levels" (Dugin, 2011).

In view of the foregoing, the world actively develops due to a unified system of information interaction and control. Despite the growing role of political and legal restrictions in the use of information, it is obvious that information security should be gradually

formed at the state and interstate levels. The need for regional and interstate interaction in the field of information exchange (scientific, cultural and technological) does not exclude but strengthens control over the collection, assembling, structuring, storage and use of information at the national level. History is replete with examples where information was lost on tangible media (the burning of the Alexandria Library (Watts, 2017), the destruction of books in during the Chinese era of Legalism (Chan, 1972), the loss of books and other monuments of Zoroastrianism during Tatar-Mongol raids) either randomly or deliberately. In this regard, the establishment of political and legal foundations of information security is a prerequisite for strengthening state principles and creating a conscious attitude of citizens to the assimilation of information and its proper use. Based on the exceptional relevance of the information security problem, in this article we aim at studying political conditions and legal bases necessary for the formation of information security in modern conditions. The objectives of the study are as follows: 1. We focus on certain regions in the world that remain trouble spots due to their years-long

478

conflicts involving several parties. 2. We consider various aspects of information security related to the independent actions of countries and civilization processes in the formation of global information space. 3. We analyze individual documents, actions and processes related to the formation and development of information security, determine the principles of its functioning and provide examples of such regions.

Methods

Issues related to information security are connected with the basics of human life, i.e. communication and social relations. Information forms the basis of communication where the issue of its use is decided at the input and output. Based on some information, decisions are made (even political ones). The use of system analysis will allow investigating the nature of the information used at all levels of political management in the modern period. For this purpose, such analysis comprises information factors that directly affect political decision-making: information on natural resources, human capital and the development of science branches, education and culture.



In addition to factual data in the above-mentioned spheres, this analysis also includes conceptual approaches based on abstract logical analysis to assessing basic informational characteristics. The nature of political management having an available information base is determined by historical traditions and socio-political innovations. In turn, this management system relies on the conceptual and basic foundations adopted in a particular society. Every political organization seeks to improve its state system. On the contrary, the social environment also makes numerous demands on the foundations of any political system. There is no single approach to the analysis and systematization of political systems because of their diversity. As a result, there are difficulties in assessing the role of information resources in state management. A possible solution is to divide countries into groups according to certain criteria: for example, the development of information society, the use of technologies in the analysis of information and its use in political processes. System analysis gives the opportunity for such an assessment. In addition, system analysis of the legal framework related to the concept of

479

information security is used to solve the problem under study.

Results

Before determining the main directions of forming information security, it is necessary to understand what kind of information requires special protection at the state level. Depending on the historical period of social development, this information can be of different types. The nature and content of information is connected with the foundations of each state, including border security, internal stability, economic power and ideological unity of its citizens. State power as a scientific category has a clear definition. Many analysts (Soifer, 2013) considered the issues of state power in their interconnection with other components of state power. Thus, it is difficult to determine the nature and content of information subject to state security once and for all. However, "states remain the basic security actors in international relations, and this means that deepening our knowledge of national security in contemporary circumstances is vital. This is especially so since state capacities in identifying, categorizing and responding to harm have become



stretched by globalization, advancements in technology and the rise of a host of threats, from transnational actors to natural disasters" (Sussex et al., 2017). Consequently, the concept of state security and its component (information security) are constantly changed and improved. However, there are unshakable principles of state existence associated with its territorial integrity and civil peace within its territory, which do not change from century to century. The specific manifestation of these indicators is connected with typical characteristics of the period in which a certain state develops.

We do not dwell on the modern world order (Baylis et al., 2016) but it is clear that inter-state relations are based on generally accepted principles that are reflected in several international documents. The further strengthening of political stability in this area is determined by the balance of international forces fighting for leadership on a global scale. Their priorities mostly define the establishment of state security in each country of a particular region. In addition, there are global problems that directly affect the world order and

480

relations between countries and regions (What are the 10 biggest global challenges? 2016).

We can emphasize only general requirements for information directly related to state security and affecting its provision. The source notes that "'information' means any original or copy of documentary material irrespective of its physical characteristics, and any other tangible or intangible material, regardless of the form or medium in which it is held. It includes, but is not limited to, records, correspondence, facts, opinion, advice, memoranda, data, statistics, books, drawings, plans, maps, diagrams, photographs, audio or visual records, documents, emails, logbooks, samples, models, and data held in any electronic form. 'Information of public interest' refers to information that is of concern or benefit to the public, not merely of individual interest and whose disclosure is 'in the interest of the public', for instance, because it is useful for public understanding of government activities" (The Global Principles on National Security and the Right to Information, 2013).

Thus, the content of information can be determined by its

various types and affect its safety and relevance in politics. Let us consider the socio-political foundations of information security with due regard to the above-mentioned content and types of information. A question posed in the broadest sense makes us analyze general approaches to socio-political foundations. We prove our conclusions with concrete facts. What determines possibilities and conditions for the acquisition and preservation of information, as well as requirements for its content and quality? It is difficult to answer this question unequivocally. After all, each state has its own resources, political regime, historical stages and features of socio-economic, demographic and cultural development. Each state is integrated into the world community in its own way and has its own authority as an international actor. It is important to consider the role of this state in a particular region and throughout the world. Therefore, only powerful states can effectively use information as an integral element of their state security. Each country forms and improves its own political and legal framework for determining the content of information that should be stored (Developing National Information

481

Security Strategy for the Kingdom of Saudi Arabia, 2016).

Depending on the political regime and actions of authorities, information might be public or concealed. Information security stipulates that information should be protected not only from external threats but also from citizens of a particular country. In this case, the ultimate goal is to ensure national security (protection against an external threat). At the same time, there are anti-democratic, totalitarian and authoritarian regimes, which create artificial obstacles to the receipt of information by ordinary citizens. The reason is the directed impact upon human consciousness and state desire to maintain central power through brainwashing. A similar policy was conducted in the past when the otherwise-minded were executed, books were burned, advanced scientists were persecuted, etc. (Martínez, 2018). Information can be associated with different spheres of public life, natural resources, information technologies, scientific experiments, etc. Depending on the importance of information, it is possible to develop certain protective measures.



We should highlight such a form of concealing information as the creation of myths (false information). This political means is used in confrontations between countries or blocs. For example, information played a crucial role during the Cold War when different authorities tried to influence the mass consciousness of their citizens and the public opinion of the world community (Cold War History, 2019). Another example is the tactics of the Soviet government regarding local conflicts within the country (Mammadov, 2012). Nowadays it is a common method of protecting statehood and some data under the guise of distorted or inadequate information. There are many opportunities for applying this method since information and communication technologies are developing and their impact on the general population is expanding every day. Combating information campaigns with the help of other information has become an integral part of political technologies within one country and beyond its borders (Darrell, 2017). One more form of information warfare is the concealment of information or its destruction. We have already discussed this form at the beginning of the article.

482

We should note that the destruction of evidence (undesirable information) sometimes changed the course of history in a particular region. Random findings can shed light on the darkest periods of history when the knowledge of the truth was punished in the cruelest way (inquisition, totalitarian regimes, etc.).

Thus, there are many possibilities of creating information security and this process can go in the direction of keeping the necessary information under the seal of secrecy and its intentional distortion. It all depends on the political strategy chosen by the state, its leadership, priorities, internal and external political forces, groups, etc.

The main directions for forming the legal basis of information security

Now let us consider the legal foundation of information security. The preservation of information and the creation of the information environment favorable for the socio-economic and political development of any country are possible only on a strong legal basis. International law is also important in the field of preserving, transferring and using information. However, the legal framework of any social phenomenon that requires the constant attention of



society cannot accurately reflect all changes that occur in real life. In other words, the existing law lags behind reality. The modern civilization that has moved to the level of information society determines the high rate of changes in the legal framework regarding the preservation and protection of information. It is noteworthy that "information, as a reproducible resource, becomes an object of sale and purchase and a source of long-term economic growth". There are eight characteristics of the modern information society: "unique knowledge, strengthening the role of entrepreneurship, digital technologies, creative highly qualified specialists, the growth of the global online population, the lack of ICT skills, the rapid development of the mobile world, the lack of a unified methodology for measuring ICT skills" (Isaev & Vasilyeva, 2019). Stages of expanding the use of information opportunities indicate that information society has already been formed. The ability to adapt to the outside world and establish mutually beneficial relations becomes an obvious advantage of using information in its different forms.

The world community seeks to unite efforts to combat violations of

483

information security and its use, which causes tense situations in different spheres of life (cybercrime, the use of information and communication technologies in terrorist acts, the formation of certain stereotypes in the public mind through social networks, the development of various political technologies aimed at increasing social tension in certain regions of the world, etc.). Currently, several international treaties unite efforts in the legal regulation of information exchange, use and preservation of information (Convention on Cybercrime, 2001). Furthermore, their number is growing and their content is being improved. Ensuring the safety of information and providing conditions for the use of information are also regulated by legislative acts at the level of each state. These acts vary from region to region and from country to country, which is associated with some historical prerequisites for forming statehood and political structures, as well as ensuring socio-economic development. There are contradictions between international conventions on information security and some national laws. However, scientists believe that there is a unified concept for the formation of an international legal



base in the field of information security. It is only necessary to adopt the relevant laws on this basis, i.e. "the unified concept of provision of the international information security has developed at the global and regional levels, which needs legal instruments for its implementation at the global level" (Talimonchik, 2019). To overcome the above-mentioned contradictions, specialists hold forums and international meetings. At the same time, it is clear that the fight against the misappropriation of information, its distortion and use for illegal purposes, including for overthrowing governments and escalating international and regional conflicts, have not been fully studied. In this regard, it is necessary to strengthen international law and order and increase the role of authoritative international organizations in ensuring information security (Sloss, 2009).

Discussion

The issues of information security are crucial for states and the entire world community. Using information technologies, information terrorists hack servers, transmit confidential information to social networks, attack sites of transnational corporations, etc. Thus, it becomes

484

difficult to preserve information and use it for the benefit of people. In this regard, it is unclear whether scientists rightly suggest only improving forms of information protection and strengthening the current legal framework, i.e. "improving government security practices, providing funding for cybersecurity programs and initiatives, restricting public disclosure of sensitive government cybersecurity information, promoting workforce, training, economic development" (Cybersecurity Legislation, 2018). This issue should be considered on a broader scale. These processes are conditioned by the socio-economic interests of individual countries in the distribution and redistribution of resources, their focused efforts to achieve greater power in some region and around the world.

For such needs, countries launch a multi-purpose process to undermine the enemy's power. These actions include not only economic techniques and methods but also the impact on people's consciousness through mass media and the education system, as well as the formation of new values and norms of social life. Thus, it is necessary to ensure direct information flow through various channels using



information and communication technologies, replace ethnic cultural values with the borrowed ones and transform the existing education system to bring up younger generations with a limited worldview, primitive needs and a consumer attitude to life. The social consciousness of masses forms radicalism and contempt for political values, as well as the desire to express their attitude to some issue only by extreme means.

We believe that it will be increasingly difficult to ensure information security without consolidating basic humanistic principles in the minds of people, at least most of them. It is necessary to promote democratic principles of the existence and functioning of each country, a high level of education and living standards, a set of spiritual values, with priority given to universal values. Therefore, joint efforts should ensure systematic compliance with the basic norms of international relations developed between countries and regions over the past centuries.

Conclusion

The political and legal foundations of information security were

485
 formed in parallel with state systems. Throughout history, different types of information were used in favor of state, which was reflected in the legislative framework. Since the issue of information security becomes more and more complicated from year to year, we can conclude that it is extremely relevant. Nowadays there are more possibilities of using information and exchanging it with the environment. However, the current development is likely to complicate this situation. Cybercrime rates grow higher and become one of the biggest threats to the survival of humankind. Not only individual organizations but also entire states cannot overcome it. Sometimes it is difficult to determine the hiring party behind the activities of information terrorists since modern information and communication technologies assist them in committing their crimes. In this regard, possible obstacles are the imperfection of state legislation, the instability of political regimes, the underdevelopment of management systems and the presence of a large group of people dissatisfied with the existing social system.

References:

1. Baylis, J., Smithson, S. & Owens, P. (2016). *The Globalization of World Politics: An Introduction to International Relations*. Oxford, UK: Oxford University Press.
- Chan, L.M. (1972). The Burning of the Books in China, 213 B.C. *The Journal of Library History*, 7(2), 101-108.
- Cold War History. A&E Television Networks. (2019). Retrieved from <https://www.history.com/topics/cold-war/cold-war-history>
- Convention on Cybercrime. ETS No.185. (2001). Budapest. Retrieved from <https://www.coe.int/en/web/conventions>
- Cybersecurity Legislation (2018). Retrieved from <https://www.ncsl.org/research/telecommunications-and-information-technology>
- Darrell, M. (2017). How to combat fake news and disinformation. West Monday. Retrieved from <https://www.brookings.edu/research/>
- Developing National Information Security Strategy for the Kingdom of Saudi Arabia (2016). Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository
- Dugin, A.G. (2011). *Geopolitika [Geopolitics]*. Moscow: Gaudeamus. Akademicheskii proekt.
- Fjäder, C. (2014). The nation-state, national security and resilience in the age of globalization. *International Policies, Practices and Discourses*, 2(2), 114-129.
- Isaev, A.P. & Vasilyeva, T.V. (2019). The genesis of the modern information society and the main world characteristics. *Upravlencheskoe konsultirovanie*, 8, 19-27.
- Kornblum, A.N. (1985). *Defense Intelligence College (U.S.). Intelligence and the Law: Protecting intelligence sources and methods. Unauthorized disclosures. International terrorism. Technology transfer. Intelligence and the Law: Cases and Materials (Volume 2)*, Defense Intelligence College.
- Mammadov, F. (2012). The Gorbachev factor in the Karabakh conflict. Retrieved from <http://www.visions.az/en/news/359/bc242690/>
- Martínez, A. A. (2018). Was Giordano Bruno Burned at the Stake for Believing in Exoplanets? Most historians say no, but new evidence suggests otherwise. Retrieved from <https://blogs.scientificamerican.com/observations>

- Paul, T.V., Wirtz, J.J. & Fortmann, M. (2004). *The enduring axioms of balance of power theory. Balance of power: Theory and practice in the twenty-first century.* Stanford, CA: Stanford University Press.
- Persson, G. (2017). *The War of the Future: A Conceptual Framework and Practical Conclusions: Essays on Strategic Thought*, August 11, 2017. By Gudrun Persson for NATO Defense College (NDC).
- Pompon, R. (2020). *Information security Trends and Solutions for the New Decade New Year, New Risks: What Can We Expect From the World of Cybersecurity in 2020?* Retrieved from <https://www.informationsecuritybuzz.com/articles>
- Redhead, S. & Virilio, P. (2004). *Theorist for an Accelerated Culture.* University of Toronto Press.
- Schweller, R.L. & Pu, X. (2011). *After Unipolarity: China's Visions of International Order in an Era of U.S. Decline* (2011). *International Security*, 36(1), 41-72.
- Sloss, D. (2009). *The Role of Domestic Courts in Treaty Enforcement: A Comparative Study.* Cambridge University Press.
- Soifer, H.D. (2013). *State Power and the Economic Origins of Democracy.* *Studies in Comparative International Development March*, 48(1), 1-22.
- Sussex, M., Clarke, M. & Medcalf, R. (2017). *National security: between theory and practice.* *Australian Journal of International Affairs*, 71(5), 474-478.
- Talimonchik, V.P. (2019). *Legal Aspects of International Information Security.* Retrieved from <https://www.intechopen.com/online-first>
- The Global Principles on National Security and the Right to Information (Tshwane Principles). (2013). Retrieved from <https://www.justiceinitiative.org/uploads/>
- Wall, L.S. (1972). *Alberta. Commission on Educational Planning. A Future of Choices: A Choice of Futures.*
- Watts, E.J. (2017). *Hypatia: The Life and Legend of an Ancient Philosopher.* England: Oxford, Oxford University Press.
- What are the 10 biggest global challenges? (2016). Retrieved from <https://www.weforum.org/agenda/2016/2016/01>