Published by the decision of the Scientific Council of
The Institute of Philosophy, Sociology and Law of NAS RA

The POLITNOMOS

Journal of Political and Legal Studies

2(2), 2023

YEREVAN – 2023

POLITICAL STUDIES, POLITICAL PHILOSOPHY

ESSENTIAL ELEMENTS FOR INFORMATION SECURITY: PROVISIONS AND IMPLEMENTATION MEASURES

Mariam Gzoghyan,
PhD Student at the Institute of Philosophy,
Sociology and Law of NAS RA
(email: mariam.gzoxyan.1998@gmail.com)

Abstract

In contemporary international relations, states place significant emphasis on the matters of modernization and the upkeep of information security mechanisms. It is important to highlight that with the increasing role and volume of information, the threats to information security have correspondingly grown. Consequently, safeguarding information has emerged as a foremost focal point within the domestic and foreign policies of numerous states.

Analyzing various scientific works, I consider it necessary to emphasize that in the past, security was primarily associated with military aspects in both scientific and political contexts, today, there is a growing focus on the non-military dimensions of security. As a result, states and international organizations are now tasked with ensuring collective security across various domains, including politics, economics, society, ecology, and the military. Moreover, according to the nature of their regime, countries solve the problem in different ways. Some close the information field, banning even the use of social networks, others are looking for more liberal methods (Mkrtchyan, 2017).

Advancements in information technology and telecommunications have become an important tool for promoting their interests and goals in international exchanges, so states spare no effort in establishing professional "information armies" and secure information infrastructures. Recent global experience demonstrates that the influence of information flows can be a *powerful weapon for states conducting actions against their adversaries. States lacking the capacity to counter this weapon may find themselves at a disadvantage.*

Starting from a political science perspective, it emphasizes the necessity of the private sector and state institutions to collaborate in countering various threats in the field of information security.

Keywords: international relations, information security, modernization, focal point, domestic and foreign policies, telecommunication.

Ensuring Information Security as a Crucial Factor in the Republic of Armenia's Ongoing Modernization Efforts

In reference to information security in the Republic of Armenia, it's important to acknowledge that ongoing societal developments underscore the growing significance of the information sector. The information sphere encompasses various entities involved in collecting, processing, distributing, and utilizing information, along with information subsystems. It also constitutes a framework for regulating public relations that arise during these processes. This sector, as mentioned, plays a vital role in coordinating and regulating public life, significantly impacting the political, economic, military, and other components of Armenia's security.

In the contemporary era of the post-industrial or information society, marked by profound transformations in the realms of science, technology, and production, states are confronted with the imperative to address modern global systemic challenges. Among these, the issue of information security stands out as a critical concern, as it pervades all aspects of human activities.

Individual interests in the information sphere encompass various aspects, including the exercise of a person's and a citizen's constitutional right to access information for lawful activities. These interests also extend to personal development in physical, spiritual, and intellectual dimensions, as well as access to information related to environmental changes and the safeguarding of personal safety through information protection.

The information society is characterized by the development of social and industrial relations where the majority of products are a result of high technology and the creation and sale of information products. This means that intellectual work by citizens is a primary driver of these products (Emelyanov & Streltsov, 1999).

In the information sector, the interests of society encompass various crucial aspects. These include safeguarding individual interests within this sector, fostering democracy, establishing a legal and social state, promoting social consensus and tolerance, preserving the spiritual and historical-cultural heritage of society and its diverse segments, nurturing and developing national values and traditions, and reinforcing national identity. Additionally, it involves strengthening the foundations of society, such as moral and psychological development, language, and the role of the national church. Furthermore, it's about ensuring the information connectivity that binds the state with its diaspora.

In this context, the perspective of psychologist K. Nalchajyan is particularly significant. He suggests that the diminishing presence of national psychology and a weakening sense of self-awareness in Armenia pose a genuine threat to the nation's identity. This, in turn, has implications for increased emigration and the dilution of cultural and educational values.

When considering the modernization of national interests, it becomes clear that the foundational pillar of national interest lies in vital interests. These vital interests revolve around ensuring the fundamental conditions for the survival and functioning of the interested entities, as well as the safety of life activities. The principal components of this axis include safeguarding the state's territorial integrity, guaranteeing border inviolability, preserving political independence and sovereignty, meeting the essential economic requirements of society, and safeguarding unique national and nationalist traditions.

In line with national interests, state policy is tasked with the responsibility of guaranteeing the security and progress of both the state and society. It is crucial not only to comprehensively and transparently assess these interests but also to possess and mobilize the necessary resources to facilitate the actualization of these national interests.

In the contemporary world, the power potential of a state undeniably holds a significant role. However, various crucial factors influence the actualization of national interests. Among these factors are the stance and interests of the international community, the extent of democratization within the state, the level of civilization development within both the state and the nation, and more (Ghevondyan, 2011, p. 19).

From my perspective, in the realm of state policy concerning national interests, the comprehensive assessment of the collective power of the state is particularly crucial. It serves as a key component in the comparative analysis of individual states, highlighting their distinctive attributes.

As a nation situated within a complex geopolitical region, the Republic of Armenia is actively engaged in information influences and flows. Today, we confront various challenges, including the need to mitigate the adverse effects of threats to Armenia's national interests within the information sector. Additionally, there is a growing necessity to devise new and well-considered initiatives for the secure pursuit of our national and state objectives. This entails crafting an information policy strategy aligned with contemporary information dynamics and guaranteeing the information security of the Republic of Armenia, both at home and on the international stage.

At present, the Republic of Armenia is confronted with several information security challenges, including the dissemination of false and distorted information, international terrorist activities in the information domain, the propagation of anti-Armenian false information by international information sources, disruptions to the regular operation of Armenia's information and telecommunication systems, and inefficiencies in information storage.

It's important to note that the Republic of Armenia has several legal documents related to the field, including Laws of the Republic of Armenia:

1. "On State and Service Secrets" (1996)
2. "On Freedom of Information" (2003)
3. "On Archive File" (2004)
4. "On the Protection of Personal Data" (2015)
5. "On Electronic Document and Electronic Digital Signature" (2005)
6. "On Electronic Communication" (2005)
7. "National Strategy of Combating terrorism" (2012)
8. "The concept of Formation of Electronic Society" (2010)
9. "On Mass Media" (2003)

These legal documents provide a framework for various aspects of information and data management within the country.

The current state of information security in the Republic of Armenia still falls short of meeting the modern demands of both society and the state. There is a pressing need for a limited number of well-defined regulatory laws and acts that will foster the stable growth of the sector and ensure a secure future. Information security, like in all nations, including Armenia, is an integral component of the country's national security.

As of now, information security matters are regarded as one of the most critical and perilous challenges for Armenia, encompassing both technical and content-related aspects. We think that our republic should develop a clearer vision and strategy for safeguarding information security.

The existing conditions of political and socio-economic development in the Republic are giving rise to conflicts between the growing demands of society for the free exchange of information and the necessity to maintain certain regulated constraints on information dissemination.

The underdeveloped and contentious state of legal regulation in the information sector has resulted in significant adverse consequences. Inadequate legal norms governing relationships in the foundational aspects of the constitutional order, the protection of citizens' rights and legitimate interests, and the constitutional limitations on mass information freedom to safeguard the country's defense capability and state security significantly complicate the task of achieving a necessary balance between the interests of individuals, society, and the state in the realm of information. This also hinders the development of competitive Armenian information agencies and media outlets in the country.

It is essential to undertake efforts directed towards the legal development of public relations and the resolution of conflicts in the information sector. This includes the formulation of clear state programs designed to ensure information security, the establishment of criteria and methods for evaluating the effectiveness of information security systems and measures, and the safeguarding of information technology and its development.

So, to summarize the above, the primary essence of the concept of “information security” is to safeguard information: protecting entities engaged in information exchange from adverse influences and satisfying the informational needs of social actors. This can primarily be achieved by studying the detrimental effects of information technologies on society and its members, which will aid in mitigating their harmful consequences and creating a secure information environment.

The Security Challenge and Response System

The concept of security, despite its apparent simplicity, is exceedingly comprehensive, encompassing virtually all aspects of societal and individual life. It is not coincidental that one can encounter diverse interpretations and definitions of this concept in literature. For instance, a common definition often found is: “National security is the ability of a nation to meet the requirements for self-defense, self-reproduction, and selfimprovement while preserving its fundamental values with the least possible loss”. While this definition is quite encompassing, it can be somewhat static and may not fully capture the nuances of a changing environment. Consequently, it's valuable to also consider the formulations of Arnold Toynbee (1889-1975), who made significant contributions to the development of security philosophy (Toynbee, 1987).

In attempting to summarize Toynbee's classical perspectives, the security of civilizations, states, societies, and even individuals hinge on their capacity to navigate within a complex system of challenges and effectively respond to them.

Toynbee's well-known assertion highlights that the downfall of civilizations often stems from their inability to respond adequately to the challenges they face. It's worth noting, however, that challenges, in certain situations, can also be viewed as a positive factor because they serve as tests that assess the robustness of the security system. To meet challenges successfully, they prompt the mobilization of spiritual, intellectual, military-political, and material resources within the public (Toynbee & Myers, 1959).

It is evident that a weak security system and the underestimation of its significance inevitably lead to severe consequences. These consequences may include the loss of statehood, the displacement of populations, genocides, internal and external conflicts, multifaceted crises, erosion of material, spiritual, and moral values, the disruption of traditional ways of life, the decline of ethics, degeneration, and ultimately, destruction.

The issues related to information security are progressively escalating and pose threats at the national level.

Toynbee's observations are also applicable in the realm of information technology (IT). The scope of IT is at times narrowly defined, but it is, in fact, a broad concept encompassing everything related to:

- The challenges of effectively developing, managing, and securing the spiritual, psychological, intellectual, knowledge, and educational aspects of the nation, state, society, and individuals.
- The challenges of effectively developing and securing information technology systems for the state, society, and individuals.

Based on these and similar perspectives, various definitions of information security have been proposed in professional literature. For instance, A. D. Ursul defines information security as the state of safeguarding the essential facets of life from harmful information effects (Ursul, 1990).

In accordance with the principles of Toynbee's security philosophy and underscoring the paramount role of scientific, educational, and technological resources, as well as the collective competencies of the public in matters of security, information security can be defined as follows: "Information security is the capability to safeguard and advance the welfare of the public by establishing the requisite knowledge and technological resources within the state and society, in response to the challenges posed by information".

Information Conflict Technologies

As Henry Kissinger, the former national security adviser to the U.S. President, pointed out, discussions about the information age often focus on its significant societal, economic, and political implications, considering it a great intellectual revolution in history. However, its impact on international relations is less frequently discussed, except for acknowledging the global capabilities of modern communication channels. Even then, the focus tends to revolve around numbers and the speed of information transmission. What's often overlooked is those international relations, and consequently the course of history, are influenced not just by the number of people with access to information but, more importantly, by how information is perceived. Given that the volume of available information typically surpasses our capacity to process it, the gap between information and knowledge, and even more so between knowledge and wisdom, continues to widen.

In recent decades, the Republic of Armenia and the Republic of Artsakh have actively engaged in information warfare. These Armenian republics have accumulated extensive experience and knowledge in countering Azerbaijani information policies. However, the ever-evolving means of communication and the escalating propaganda efforts by adversaries necessitate the ability to keep up with the changing times and respond effectively when required.

The concept of “information warfare”, which emerged in the late 20th century, has swiftly captured the attention of many authors. Some notable works in this area are included in educational materials, such as M. Libiki's “What is information war?” G. Pocheptsov's “Information wars, basics of military-communication research”, G. Harutyunyan's “Problems of RA information system development in the context of national security”, and others.

In 1976, the Western scientist Thomas Rona used the term “Weapon Systems and information war” in his report for the “Boeing” company, primarily focusing on communication systems. Rona stressed that the adoption of new communication technologies in the military domain requires a new level of integration. It's essential to prevent information leaks that could provide the adversary with advantages in communication technology. He viewed information warfare as a means of safeguarding against potentially dangerous information leaks from the enemy while simultaneously deploying information flows targeted against the adversary (Rona, 1976).

Specialists in information warfare typically refer to a system of actions aimed at influencing the information and information infrastructures of an adversary while safeguarding one's own information and information systems. This definition highlights that information warfare encompasses not only information attacks but also information protection and security. The concepts of “information warfare” and “information security” are closely interconnected. Information warfare is the entity to disrupts, disables, or destroys information security as the target. Information security, on the other hand, can be defined as the protection of the information environment of society and government bodies, including the state. It's important to note that information security encompasses both the safeguarding of the information environment of society and the state, as well as the security aspects of information-technical systems.

According to the famous information security expert, I. Panarin, information warfare has been a longstanding element of global politics throughout human history. It has been the primary means of attaining spiritual, political, financial, and economic power in the world.

M.V., an analyst at the Information Security Institute of Lomonosov Moscow State University and a Doctor of Technical Sciences, S. Rastorguev, defines information warfare as the conflict between states that employ information technology and technical resources.

Information Weaponry

In a broad context, this term refers to the tools and methods used to influence information directed at an adversary to exert control and alter their strategic and tactical perspectives in a favorable direction for the influencer. In a more specific sense, information weaponry encompasses a comprehensive set of methods and technological means designed to gain control over the information assets of a potential adversary. This includes disrupting their information systems, disabling them, accessing or altering the data they contain, and introducing advantageous information (or misinformation) with a specific purpose.

The varieties of information weaponry and the techniques for their utilization are continually advancing. This evolution is inherently linked to the development and application of new concepts in information warfare.

Employing information weaponry necessitates more than just a thorough understanding of the enemy's technical capabilities. It's equally crucial to possess deep knowledge of the ethnopsychology and cultural characteristics of the intended individuals and populations, as these factors significantly influence how people absorb and interpret information, ultimately shaping their decision-making processes.

Mass media plays an important role in information warfare. Various countries, equipped with cutting-edge technological capabilities and enjoying global recognition, broadcast their specific informational narratives during various international events. They engage in information collection, processing, and analysis, and then deliver the news to their intended audiences with a particular direction or bias. The methods and opportunities employed in information conflicts can influence the actions of individuals, society, and even states.

In the current era of extensive information conflicts, where “the powerful set the rules of the game” and seek to impose their values on others, the significance of this function becomes evident in the context of globalization.

When discussing “information warfare”, it's important to recognize that it is not a static or permanent set of activities; it is continually evolving and changing. During information warfare, alterations in its various components commence and persist, making it challenging to accurately predict how the process will unfold with its multitude of elements.

The theoretical foundations and philosophy of military strategies and indirect operations (in which information operations play a crucial role) were comprehensively developed by the great Chinese thinker Sun Tzu in the 4th century BC, according to some sources, or in the 6th century BC.

Sun Tzu, the legendary military strategist of ancient China, is renowned for his influential work, “The Art of War”. He was a master of “soft power” and is often regarded as the precursor to the concept of “blitzkrieg”. His preferred approach was to secure victory without engaging in combat, or if necessary, to win with minimal battles.

His famous treatise, “The Art of War”, forms the foundation for various theoretical researches, and its principles are widely applied in practical studies. Sun Tzu believed that warfare should only be pursued when all other means of defeating the enemy have been exhausted. According to his philosophy, the ultimate victory is achieved through diplomatic methods without resorting to military operations. To achieve this, he emphasized the importance of active diplomacy, the dismantling of enemy alliances, and the disruption of their strategic plans, a strategy often described today as the use of “soft power”.

It's no coincidence that the principles outlined by Sun Tzu are widely spread today, with numerous references to his work in hundreds of scientific articles and publications. Furthermore, modern military and specialized service academies typically include the teachings of Sun Tzu as part of their curriculum.

A noteworthy aspect of Sun Tzu's approach is the emphasis on the knowledge possessed by a military leader as the primary and decisive factor in achieving victory. This perspective aligns well with contemporary concepts related to information strategy, where knowledge and intellectual resources are considered fundamental elements in the realm of information security. Therefore, Sun Tzu can be rightfully regarded as the pioneer of the philosophy of information security.

The ideas and aphorisms contained in Sun Tzu's work are remarkably concise and insightful. Here are two of them presented in a somewhat paraphrased form:

- “If you know your enemy and know yourself, you will win hundreds of battles. If you know yourself but not the enemy, each victory will be followed by defeat. If you know neither yourself nor the enemy, you will lose all battles".

- "War is a realm of deception. If you have the ability, make your opponent believe you don't. If you employ a tactic, make it appear as if you're not. Even when close to your adversary, create the illusion of being far away. When you are far away, make it seem as if you are near".

Sun Tzu also emphasized his view that war is an undesirable evil that should be minimized whenever possible. He likened war to fire, noting that those who refuse to put down their weapons will ultimately suffer from their own actions. He advocated conducting wars swiftly to prevent economic losses, as he believed that prolonged conflicts rarely brought benefits to a nation. He famously stated that achieving victory in every battle is an unrealistic goal, and those who distinguish themselves in defeating their enemies should seize the moment until the threat subsides.

Furthermore, Sun Tzu's wisdom highlights the importance of avoiding mass killings and atrocities in warfare. He recognized that such actions could provoke resistance and provide the enemy with an opportunity to turn the tide of the conflict in their favor.

Generalizing Sun Tzu's concept, it becomes clear that indirect, often purely informational actions are favored in the battle against the enemy. The objective is to "undermine the strengths of the enemy, implicate their prominent figures in illicit activities, subject them to public ridicule, and collaborate with the most unscrupulous individuals".

It's worth noting that one of the foundational principles of Sun Tzu, "create confusion and chaos in the opponent to defeat them", serves as the basis for the modern concept of so-called "second-generation" information warfare developed by American think tanks. The value of theoretical works is often best realized when their ideas are put into practical application. From this perspective, it's remarkable that Sun Tzu's strategic concept, in alignment with the Chinese psyche and way of thinking (which is significant), has been actively employed and utilized throughout China's history.

The attention to past knowledge and, most significantly, their preservation and development have played a vital role in the establishment of a unique yet highly effective Chinese national security system. In this regard, it can be viewed that Sun Tzu performed a task that is like modern “think tanks”, whose purpose is to translate theoretical knowledge into practical application, particularly in the realms of politics, military strategy, and information warfare.

It's noteworthy that China historically engaged in very few wars beyond its borders, instead opting to resolve issues with its neighbors primarily through diplomatic and economic means. A prime example of these approaches is the ancient “Silk Road”, which connected East Asia with the Mediterranean region and is currently experiencing a revival.

This strategy significantly helps preserve human resources. It's insightful to compare the demographic statistics of two former empires, China and Mongolia (the latter aimed at territorial conquest). China still employs Sun Tzu's strategic principles in its policies today, contributing to its continued strength.

Addressing Infogenic Threats: International Control Measures and Responses

Throughout history, one of the primary concerns of every state has been safeguarding the security of the nation. When infogenic actions target the interests of rivals or conventional adversaries, they should be viewed as challenges. Infogenic challenges primarily fall into two categories.

Spiritual and ideological infogenic threats, which are aimed at the nation, society, and individuals, emerge within the influencer's interests.

These threats seek to:

- Disrupt public consciousness, at times even at the subconscious level, affecting spiritual and national values.

- Alter the political and educational orientations of society and individuals, thus influencing the state (often referred to as the “civilizational code”).
- Reduce the general intellectual and knowledge resources of the society and the state, thereby restricting the development opportunities of the affected society.

Infogenic threats of a technogenic nature are aimed at the information technology systems that coordinate the activities of individuals, society, the nation, and the state. Sources of infogenic threats can be both external and internal.

In the case of the Armenian community, external sources of informational threats may include:

- Countries and organizations that compete with or oppose Armenian states and society.
- Countries and organizations pursue their interests while neglecting the interests of Armenian states and the public, including political and economic partners.
- Chaotic information flows circulating in the global information field, not specifically targeted against the Armenian community but negatively affecting public and individual consciousness.

Infogenic challenges can also pose internal threats within the Armenian community. These threats may arise from:

- Political, social, and economic organizations, as well as mass media outlets located in Armenia but influenced by foreign sources, whose activities do not align with the interests of the Armenian community.
- Political, social, and economic organizations, companies, state bodies, and mass media operating with domestic private and state resources, but lacking clarity on the national interests of the Armenian community. Consequently, such entities can pose an informational risk to the Armenian public due to unintentional or political-ideological misalignments. Some instances of such

actions are occasionally described as “information warfare” against one's people.

- Additionally, the identification of infogenic challenges, their proper coordination, and analysis enable an understanding of the strategy of a conventional opponent or competitor, as well as the methodology of its implementation. Furthermore, presenting infogenic threats to the public with appropriate explanations and “informational support” mobilizes both society and the state, facilitating an adequate response to the challenges at hand.

State security encompasses several crucial aspects, including:

- Military-political security
- Socio-economic security
- Information security.

These components are interconnected, and the boundaries between them are highly conventional. Neglecting any one of these three elements can render the state's security incomplete. While the military sphere has traditionally been considered the top of the security hierarchy (often equated with the concept of “security” itself), contemporary developments compel theorists to move away from traditional approaches. They emphasize the significance of non-military aspects of society, leading to a reconceptualization of the security system. In this new paradigm, the security system resembles a network, with information security at the center, interconnecting the other components of security (Harutyunyan, 2002).

In the context of the “information society”, where the volume of information has significantly changed and increased, a new diplomatic landscape has emerged. While traditional diplomatic methods still hold their importance, there is an urgent need to adapt to new approaches. In the past, it was primarily diplomats who possessed extensive knowledge of events occurring in various parts of the world. However, today, virtually every citizen can access relevant information through the Internet.

Russian Foreign Minister S. Lavrov's remarks on information diplomacy are worth remembering. He emphasized the importance of utilizing various forms of diplomacy for different scenarios. In today's world, the role of the media is paramount, making information diplomacy a more favorable approach compared to information warfare.

Information diplomacy serves as a vital and nuanced instrument for gaining widespread international acknowledgment. It advances foreign policy objectives and effectively communicates information to both the public and political leadership through mass communication channels. Representatives from each country's foreign policy apparatus employ the tools of information diplomacy to achieve their objectives.

Information Security in Armenia: Current Challenges and Concerns

In recent times, the Republic of Armenia has taken several measures to enhance its information policy and information security. These efforts include the establishment of a legal framework for information security.

The National Assembly of Armenia has ratified the Council of Europe Convention “On Cyber Crimes” along with its additional protocol “On the Criminalization of Racist and Xenophobic Acts Committed Using Computer Systems”.

Furthermore, ongoing work is aimed at developing legal regulations governing public interactions within the information sector and refining legal practices.

Nevertheless, an evaluation of the state of information security in the Republic of Armenia reveals that it has not yet reached the contemporary expectations of both society and the state. The ongoing political and socio-economic developments in the country give rise to tensions stemming from the increasing demands for the free exchange of information within society, while simultaneously necessitating the preservation of specific regulated constraints on information dissemination.

The underdeveloped and contentious state of legal regulations governing public affairs within the information sector results in significant adverse outcomes. The insufficient legal framework for managing relations related to the foundational constitutional order, safeguarding citizens' rights and lawful interests, and the potential constitutional limitations on the freedom of mass information intended for preserving the nation's defense capabilities and state security, all contribute to the challenging task of striking an appropriate balance between individual, societal, and state interests within the information realm. Furthermore, this situation makes it difficult for Armenia to support the growth of competitive Armenian information agencies and media in this area.

The insufficient protection of citizens' right to access information and the deliberate distortion of the information they receive can lead to public dissatisfaction, sometimes resulting in social and political instability.

Furthermore, the rights to privacy, personal and family secrets, and the confidentiality of correspondence, as established by the Constitution of the Republic of Armenia, lack the necessary legal, organizational, and technical measures. The protection of data, including personal information collected by government and local authorities, remains insufficient.

The field of information, telecommunications, and communications has experienced a significant reduction in its skilled workforce due to the mass emigration of qualified professionals.

Regulatory and Administrative Mechanisms for Controlling the Information Space

The power of mass media to shape public opinion, affect mental states, and influence behavior poses a significant challenge to all societies. These challenges can become severe threats, with implications for both national and information security. Effectively responding to such threats often requires the strategic use of counter-agitation, counter-propaganda, and revealing deceptive information tactics. Concern arises in situations where information campaigns are organized by hostile states and organizations, with the intent of destabilizing and weakening the targeted society. Notably, the creation of unfriendly mass media content in our modern era often involves various non-governmental organizations (NGOs). This complex landscape sometimes necessitates the application of administrative and legislative measures as the most effective means of protection.

Today, the Internet serves as a powerful tool in propaganda, playing a significant role in ongoing conflicts. The Azerbaijani State Propaganda Machine, under the guidance and sponsorship of President I. Aliyev spares no effort to spread anti-Armenian propaganda across the digital landscape. Azerbaijan is steadily expanding its online presence by taking advantage of the growing number of news websites that actively propagate misinformation and engage in the dissemination of propaganda against Armenia.

The Republic of Armenia (RA) currently faces a range of information security challenges. These challenges encompass the dissemination of false and distorted information, as well as international terrorist activities within the information sphere. Furthermore, there is a notable presence of anti-Armenian false information disseminated through international sources. In addition to this, there are concerns about actions that could undermine the Armenian national and cultural identity, as well as intelligence operations conducted by foreign entities. These challenges are compounded by disruptions in the regular functioning of information and telecommunication systems in the RA and inefficiencies in maintaining information resources. These multifaceted problems represent critical information security threats in the context of Armenia's current situation.

In summary, it's important to emphasize that information security in Armenia is a fundamental aspect of the country's national security strategy. It directly influences the protection of Armenia's national interests across different sectors of society and various aspects of the nation's daily life. The requirements for ensuring information security in Armenia are consistent across all domains.

Conclusion

In conclusion, our study has led to the following key findings:

- In today's information-driven society, information has taken on new significance, becoming a dominant value and a strategic resource. The creation, processing, and dissemination of information are crucial for productivity, power, and effective governance. Information plays a central role in shaping social and political developments.
- The 21st century stands out for its global connectivity and virtualization, initially marked by some negative aspects. One of the most significant threats in this era is the rise of cybercrime and cyber threats, which endanger the stability and common progress of nations, societies, and individuals.
- Present global uncertainties have presented substantial challenges to the security and political systems of countries at various levels of development. The progressing world order is reshaping existing local, regional, and global threats. Information wars have developed into a highly dangerous manifestation of this process, often arising from inter-ethnic conflicts, deteriorating interstate relations, internal political tensions, and leading to geopolitical turbulence that upsets political and public order.

  The oversight of information security in the Republic of Armenia is achieved through legal, institutional, technological support, and extensive collaboration between state administration and local self-government bodies, operating within the boundaries defined by legislation.

- At present, Armenia faces several information security challenges, including the spread of false and distorted information, international terrorist activities in the digital realm, the dissemination of anti-Armenian misinformation through global information sources, disruptions to the normal operation of Armenia's information and telecommunication systems, and the inefficiencies in information storage.
- The online environment, shaped by the Internet and digital technologies, offers unparalleled opportunities for human communication and information exchange, making it an important factor for the development of humanity.

Recommendations

Based on the aforementioned findings, the following recommendations can be proposed:

- Amid the ongoing global changes, the emergence of a new world order, and the current uncertainties, information security has assumed a key role in shaping geopolitical dynamics. It has introduced entirely new types of threats at the local, regional, and global scales. Given these factors, we find it rational to establish a unified local network within the Republic of Armenia. This network will guarantee the seamless functioning of various aspects of daily life, even in times of crisis, thereby preventing potential disruptions to public and private sector activities.
- Recognizing the significance of ensuring information security, particularly cyber security as an integral component of national security, we recommend the

establishment of a unified center for coordinating cyber operations. This center, like the Georgian Computer Emergency Team (Cert.gov.ge), would be tasked with developing an infrastructure for the exchange of information between public and private sectors and implementing information security policies.

- It is crucial to highlight the significance of encouraging a culture of cooperation and peace as a fundamental component of Armenia's program of essential measures. The objective is to advance such a culture both regionally and globally and prioritize it on the international agenda.
- Considering these and similar considerations, we find it necessary to implement mechanisms that guarantee a consistent high-quality, and competitive educational system. This approach is founded on the principles of moral and psychological stability, especially in the face of the uncertainties associated with ongoing global developments and the emergence of entirely new security challenges.

References

Emelyanov, G., Streltsov, A. (1999). *Problemi Obespecheniya Bezopasnostsi Informacionnogo Obshestva* (Problems of Ensuring the Security of the Information Society, in Russian). Information society, № 2. 15-17.

Ghevondyan, A. (2011). *Azgayin Shaheri Himnaharcy Hayastani Hanrapetutyan Anvtangutyan Apahovman Arajnayin Mijavayrum* (The Issue of National Interests in the Primary Security Environment of the Republic of Armenia, in Armenian). Yerevan.

Harutyunyan, G. (2002). *HH Teghekatvakan Hamakargi Zargacman Himnakhndirnery Azgayin Anvtangutyan Hamateqstum* (The Main Issues of the RA Information System

Development in the Context of National Security, in Armenian). Yerevan: Noravank GKH.

HH Nakhagahi Kargadrutyuny HH-um Ahabekchutyan Dem Payqari Azgayin Razmavarutyuny Hastatelu Masin (Order of the President of RA on Approving the National Strategy of Combating Terrorism in RA, in Armenian), 16 April 2012. Retrieved October 10, 2023, from: https://www.arlis.am/documentView.aspx?docID=75353.

HH Orenqy Andznakan Tvyalneri pashtpanutyan masin (RA Law on the Protection of Personal Data, in Armenian), 18 May 2015. Retrieved 10 October 2023 from: https://www.irtek.am/views/act.aspx?aid=80783.

HH Orenqy Arkhivayin Gortsi Masin (RA Law on Archive File, in Armenian), 8 June 2004. Retrieved October 10, 2023, from: https://www.irtek.am/views/act.aspx?tid=174351.

HH Orenqy Elektronayin Haghordakcutyan masin (RA Law on Electronic Communication, in Armenian), 8 July 2005. Retrieved October 10, 2023, from: https://www.irtek.am/views/act.aspx?tid=171297.

HH Orenqy Petakan ev Tsarayoghakan Gaghtniqi Masin (RA Law on State and Service Secrets, in Armenian), 3 December 1996. Retrieved October 10, 2023, from: https://www.arlis.am/DocumentView.aspx?docID=26193.

HH Orenqy Teghekatvutyan Azatutyan Masin (RA Law on Freedom of Information, in Armenian), 23 September 2003. Retrieved October 10, 2023, from: https://www.irtek.am/views/act.aspx?aid=22461.

HH Orenqy Zangvatsayin Lratvutyan masin (RA Law on Mass Media, in Armenian), 13 December 2003. Retrieved October 10, 2023, from: https://www.arlis.am/DocumentView.aspx?docid=1379.

HH Varchapeti Voroshumy Elektronayin Pastatghti ev Elektronayin Tvayin Storagrutyan masin Hayastani Hanrapetutyan Orenqi Kirarkumn Apahovogh Mijocarumneri Canky Hastatelu Masin (Decision of the RA Prime Minister on Approving the List of Measures Ensuring the Implementation of the Law of the Republic of Armenia on Electronic Documents and Electronic Digital Signatures, in Armenian), 24 March 2005. Retrieved October 10, 2023, from: https://www.irtek.am/views/act.aspx?tid=29029.

Mkrtchyan, H. (2017). *"Teghekatvakan Anvtangutyun" Haskacutyan Evolyucian* (The Evolution of the Concept of "Information Security", in Armenian). Bulletin of Yerevan University D: International Relations and Political Sciences, 8 (3 (24). 55-62.

Nakhagith Hayastani Hanrapetutyunum Elektronayin Hasarakutyan Dzevavorman Hayecakargin Havanutyun Talu Masin (Project on Giving Approval to the concept of Formation of the Electronic Society in the Republic of Armenia, in Armenian), 2010. Retrieved October 10, 2023, from: https://www.gov.am/files/meetings/2010/4655.pdf.

Rona, T. (1976). *Weapon Systems and Information War*. Washington: Boeing Aerospace Company Seattle.

Toynbee, A. (1987). *A Study of History*. London: Oxford University Press.

Toynbee, A., Myers, E. (1959). *Historical Atlas and Gazetteer: A Study of History,* Volume XI. London: Oxford University Press.

Ursul, A. (1990). *Informatizaciya Obshestva i Bezopasnosts Razvitiya Civilizaciya* (Informatization of Society and Security Development of Civilization, in Russian). Social and political sciences, № 10. 28-38.