Revista Latina de Comunicación Social
ISSN 1138-5820 / No. 82, 01-20.
https://doi.org/10.4185/rlcs-2024-2134

Information Security Communications Strategy as a Prerequisite to Counteracting Hybrid Warfare: World Experience

Estrategia de comunicaciones de seguridad de la información como requisito previo para contrarrestar la guerra híbrida: experiencia mundial

Arailym Nussipova
Department of Kazakh-American University International Educational Corporation.
Republic of Kazakhstan.
arailym_nussipova@sci-academy.cc

Gulzhan Khussainova
Department of Social and Political Disciplines K. Zhubanov Aktobe Regional University.
Republic of Kazakhstan.
gulzhan_khussainova@un-nyc.net

Raushangul Kabilova
Department of Kazakh-American University International Educational Corporation.
Republic of Kazakhstan.
raushangul_kabilova@sci-academy.cc

Esenzhol Aliyarov
Association of Political Studies. Republic of Kazakhstan.
esenzhol_aliyarov@pltch-sci.com

Botakoz Nuralina
Department of Kazakh-American University International Educational Corporation.
Republic of Kazakhstan.
botakoz_nuralina@sci-academy.cc

How to cite this article / Standardized reference:

Nussipova, A., Khussainova, G., Kabilova, R., Kabilova, R., Aliyarov, E., & Nuralina, B. (2024). Information security communications strategy as a prerequisite to counteracting hybrid warfare: world experience

[Estrategia de comunicaciones de seguridad de la información como requisito previo para contrarrestar la guerra híbrida: experiencia mundial]. *Revista Latina de Comunicación Social*, 82, 01-20.
https://www.doi.org/10.4185/RLCS-2024-2134

Date of received: 23/05/2023
Date of accepted: 18/07/2023
Date of published: 21/11/2023

ABSTRACT

Introduction: The relevance of the study is underscored in response to the need for innovative tools to counter hybrid threats in the field of information security. **Methodology:** The study's methodological approach is described, highlighting the application of methods such as analysis, systematization, and comparison. The use of these methods is emphasized in conducting a comprehensive comparative analysis of information security strategies in Ukraine, Kazakhstan, and the European Union. **Results:** It is emphasized that the study's results provide a detailed insight into the current state of information security in the analyzed countries. It is specifically mentioned that recommendations for the development of information security communication strategies are a tangible outcome of the research. **Conclusions:** The conclusion highlights the importance of developing or enhancing information security communication strategies in the countries under study. It is suggested that these strategies can serve as an effective countermeasure against hybrid warfare and enemy attacks, thereby strengthening cybersecurity and responsiveness.

Keywords: Cybersecurity; Strategic communications; Security; Information; Hybrid warfare.

RESUMEN

Introducción: Se destaca la relevancia del estudio ante la necesidad de herramientas innovadoras para contrarrestar amenazas híbridas en el ámbito de la seguridad de la información. **Metodología:** Se describe el enfoque metodológico del estudio, destacando la aplicación de métodos como análisis, sistematización y comparación. Se subraya la utilización de estos métodos para llevar a cabo un análisis comparativo integral de las estrategias de seguridad de la información en Ucrania, Kazajstán y la Unión Europea. **Resultados:** Se enfatiza que los resultados del estudio proporcionan una visión detallada del estado actual de la seguridad de la información en los países analizados. Se menciona específicamente que las recomendaciones para el desarrollo de estrategias de comunicaciones de seguridad de la información son el resultado tangible de la investigación. **Conclusiones:** Se concluye resaltando la importancia de desarrollar o mejorar las estrategias de comunicación de seguridad de la información en los países estudiados. Se sugiere que estas estrategias pueden servir como contramedida efectiva contra la guerra híbrida y ataques enemigos, fortaleciendo la ciberseguridad y la capacidad de respuesta.

Palabras clave: Ciberseguridad; Comunicaciones estratégicas; Seguridad; Información; Guerra híbrida.

1. Introduction

Information security is coming to the fore in the national security system and the world order in the twenty-first century (Sopilko, 2022). The state, which has an advantage in media and information warfare and protection, can take the lead in the economic, military-political, and other spheres. Such a state also has a strategic and tactical benefit, regulates the economic costs for the development of weapons and military equipment more flexibly, and maintains the advantage of numerous advanced technologies.

"Information security is a characteristic of astable, sustainable public administration system, which retains its vital components when exposed to internal and external threats."

Information security is an integral part of the development of the information society, which implies the expansion of technological opportunities for information exchange (Belkin et al., 2022). It also means that all subjects of information relations (information owners and users, manufacturers of information technologies and tools, service providers, and the state) are aware of the need to implement all measures to ensure the information resources and information security of the state. Since information has a direct influence on society, it is possible to counter information threats through effective interaction between state and civil society and a high-quality communication strategy within the state and at the international level.

Important trends in the current stage of human development are the intensification of cross-border information flows and the accumulation of ways and means of information exchange that are practically beyond the control of the state. New information threats and challenges are widespread against this background that require states to respond immediately and take innovative measures and solutions. In this regard, information security and its communications strategy are becoming a priority issue on the "agenda" at the international, regional, and national levels.

Information security is part of national security and is defined as the protection of state sovereignty, territorial integrity, democratic constitutional order, and other national interests. Cybersecurity is part of information security. Information security concerns information in general, and cybersecurity touches upon information in IT systems. The development and implementation of a system of information security measures involve the following: determination of the minimum level of the information infrastructure functionality and provision of the level of functioning under crisis; determination of countermeasures under emergency if critical infrastructure is attacked; development of testing methods for security tools; improvement of systems for identifying and monitoring electromagnetic interference with critical infrastructure; strengthening the Internet infrastructure; improvement of the security of control systems, etc.

In the twenty-first century, the world faces one of the main challenges- the lack of a unified and coordinated strategy to address threats to global and national security. Strategic communications can help to meet this challenge. The current communicative situation in the world is called a post-truth situation. Even the Oxford English Dictionary includes this concept and provides the following definition: political actions and thinking "in which objective facts are less influential in shaping public opinion than calls for emotions and personal beliefs" (Oxford English Dictionary, 2022). Propaganda, "intense activity," ideology, and disinformation are the notions that can be attributed to the tools of information warfare, the purpose of which is information domination.

The world became aware of the importance of effective communication with all stakeholders only with Russia's full-scale invasion of Ukraine. The list of stakeholders is as follows: international security organizations and foreign countries (both participants in the negotiation process and outside it); governmental organizations and ministries, institutions of all branches of government; non-governmental organizations (both international and domestic); local authorities; internal audiences of security institutions. Strategic communications represent not only a trend in ensuring the security of both a country and the globalized world but also a challenge. Experts of security and government institutions who hold different position levels should learn how to implement communication strategies, perceive the position of another and coordinate joint actions accordingly, counteract destructive influences and produce positive feelings (Kordunian, 2022).

The principal definition of strategic communications was proposed in 2010 in the Military Concept for NATO Strategic Communications: "Strategic communications is the coordinated and appropriate use of NATO communications activities and capabilities - Public Diplomacy (PD), Public Affairs (PA), Military Public Affairs (PMA), Information Operations (InfoOps), and Psychological Operations (PsyOps), as appropriate- in support of alliance policies, operations and activities, and in order to advance NATO's aims. Within the military structure of the Alliance, effective NATO StratCom will be achieved primarily through the existing professional military communication capabilities" (NATO Military Concept for Strategic Communications, 2010).

The key task of the communication strategy is to provide information support for the development of the state and business. The communication strategy is based on self-presentation and creative and media strategy. It is a set of the most effective tools for influencing target audiences and a particular program for using these tools. Historical and cultural resources and the position of the region leader determine the effectiveness of particular strategies in each subject. Examples of effective communication strategies for information security can be seen in countries that have faced hybrid warfare, such as Estonia and Georgia. These countries have established special divisions and programs to protect information and have carried out campaigns to raise public awareness of cyberattacks and disinformation.

Ukraine is an excellent but sad example of how failure to use strategic communications in the country has led to a threat to national security, total disinformation, information agency, and hybrid warfare. Since the beginning of the Russian aggression against Ukraine in 2014, representatives of the security and defense sector and volunteers have understood that the issue of strategic communications is an effective tool in the context of the hybrid information war waged by the Russian Federation against Ukraine. StratCom technology allows the state to be able and resistant to counteracting modern information threats.

In addition, developed countries are intensifying government activities in the direction of legislative regulation of relations in the national information space. Following this purpose, such countries endorse special regulations for the implementation of the priority bases of state information policy. The need for analysis of information security and communication strategy as a prerequisite for counteracting hybrid warfare has conditioned this study. The main sources of research were legal acts of the European Union, Ukraine, and the Republic of Kazakhstan and other official materials, including press releases, statistical data, reports of sociological research, etc. A comparative study of Ukrainian, Kazakh, and European mechanisms for ensuring information security implied studying regulatory legal acts and other legal sources of the above states, materials of sociological studies in the field of the use of television and the Internet in Ukraine, the Republic of Kazakhstan, and the EU.

The lack of studies on communication strategies of information security in the context of comparative analysis of the European Union, Ukraine as a country with a firm European integration focus, and Kazakhstan as one of the advanced countries of Central Asia makes this research relevant. The comparative analysis of the information security strategies of Ukraine, Kazakhstan and the European Union will reveal similarities and differences in the approaches of these countries and the regional bloc to information protection and countering cyber-threats. The materials of the article can be of avail to political experts, public relations specialists, PR experts, developers of communication strategies, information campaigns, and regulatory legal acts in the field of information security.

2. Literature review

As a part of the study, the authors analyzed numerous scientific works of Kazakh, Russian and foreign scholars dedicated to information security issues and their aspects, namely, information wars and the impact of information.

The following Russian researchers perfectly generalized general and special issues of the development of political communication within the global information society in their works: M.S. Vershinin, M. N. Grachev, S. A. Zelentsa, Yu. V. Irkhin, Yu. B. Yaashlev, Yu. Yu. Lectorov, E.A. Maksimova, O. A. Malalanov, M. G. Morozova, V. D. Popov, E. V. Protsentso, E. V. Rodionov, O. F. Rusaltsov, A. I. Solovev, L. P. Timofeev, A. Yu. Tsaplin, F. I. Zharkov (2009), and others.

Political experts G. Almond, M. Castells, H. Lasswell, D. Lilleker, and G. Powell, who published in English, dedicated their works to the examination of methodological foundations of the study of communication science.

Information security as a concept appeared in the late 80s in the work of German scientist G. Odermann. It refers to an important information component in international security and attempts to address security issues related to information threats in a comprehensive manner. There was a tendency to openly study the problem of information security as a separate issue in the scientific literature of the Commonwealth of Independent States from the end of 1991 – the beginning of 1992 (Lipkan, 2006).

Notably, there is no single consolidated view on the concept of "information security" in the scientific literature. For example, Bogush (2005) understands the concept of information security as the security of the information environment that meets the national interests, in which internal and external information threats do not influence the formation, use, and development opportunities. Kalyuzhny (2000) considers information security as a state of security of the information space, which ensures its formation and development in the interests of the individual, society, and nation. Zharkov (2009) understands information security as the state of legal provisions and relevant security institutions that guarantee the constant availability of data for strategic decision-making and the protection of the country's information resources. Kormych (2004) holds information security is the protection of the rules established by law, according to which information processes take place in a country, ensuring the conditions of existence and development of a person, society, and state guaranteed by the Constitution.

In his work "Information Warfare", Winn Schwartau (1996) investigates information wars, cyber threats and the impact of information on states and organizations. The author analyses the technological, social and political aspects of information wars and proposes strategies to ensure information security. The book "Russian Roulette: The Inside Story of Putin's War on America and the Election of Donald Trump" by Michael Isikoff and David Corn (2018) explores Russia's involvement in the 2016 US election and the use of information operations to influence public opinion and political processes. It provides a detailed overview of the tactics and strategies used in information impact. Clarke and Knake (2011) consider the growing threat of cyberwarfare and the impact of information on national security in "Cyber War: The Next Threat to National Security and What to Do About It". The authors analyze examples of cyber-attacks and information operations, as well as suggest strategies and recommendations for protection against them.

Cavelty (2008) considers the role of communication in information security in the context of civil-military relations. In her book "Securing the Homeland: Critical Infrastructure, Risk, and (In)Security", the author explores how different parties (civil and military) interact and exchange information about cyber-threats and security activities. In their work "Digital Diplomacy: Theory and Practice", another important research researcher in the field of information security Bjola and Holmes (2015) discusses how governments use communication technologies to manage their ways in the international community and how these technologies can be used to counter cyber-threats.

In the paper "Communications Strategy for Information Security: From Theory to Practice", Henning Brown, Michelle Chen and Katarina Wolf discuss the methodological and practical aspects of the set of information security tools, including strategy development, choice of communication channels and tools, effectiveness evaluation and risk management. In the paper "Communication Strategy for Information Security to Build in the Digital World", Daniel Rohder and Steven Schneider consider how the information security tools can be used to build trust and improve relationships between government, business, and citizens in a digital world.

Information security is a property and attribute of the information society, the activity, and the result of human activity aimed at establishing security in the information sphere. Information security is rather a process than a state since it must take into account the future. At the same time, the objects of information security are a person, society, and the state. The subjects of information security are information in all its manifestations, including sources of information, mechanisms, and means of its creation, access, dissemination, and the consequences of its use. The subjects also involve constituent and regulatory legal and administrative-organizational norms and rules that determine the order of their formation, application, and termination (Voitovy, 2019).

In her book "Communicating Cybersecurity: Why Words Matter", Karin S. Johnson explores the importance of effective communication in information security. It provides practical advice and strategies for developing effective communication plans and messages related to information security. In his article "Strategic Communication for Cybersecurity: A Taxonomy and Analytical Framework", David S. Wall reveals the basic principles and models of strategic communication in the field of information security. The author offers a taxonomy and analytical framework for understanding and applying communication strategies in cybersecurity.

"Strategic Communications for Cyber Security: A Systematic Literature Review" by Isabel Wagner is a review of scientific articles on strategic communication in the field of cybersecurity. She analyses existing literature and highlights key topics, challenges and communication strategies that can be applied in the context of information security.

The above indicates the meaning and context of information security are so comprehensive and complex that it requires the mobilization of scholars from different spheres of science. The formation of the concept of strategic communications has passed three stages in the NATO system:

1. Strategic communications = public affairs – the function of actively leading civil society's relations with the authorities. This approach is inherent in certain national institutions but is not a common NATO standard.

2. Strategic communication is a battle of narratives (NATO's obsolete approach).

3. Strategic communications are not public affairs but an integrated form of systemic actions in the information space (NATO's modern approach).

The document "Effective Cybersecurity Communication: A Policy Brief" (Australian Government, 2016), developed by the Australian Government is very interesting in the context of effective communication in the field of cybersecurity. It discusses the importance of effective communication in cybersecurity and provides practical recommendations and examples for improving information security communication efforts.

These scholarly papers represent only a small part of the literature related to the communication strategy for information security.

3. Information security in the republic of kazakhstan

The Republic of Kazakhstan takes a leading position in terms of access to information technologies among the countries of Central Asia. Information security in the Republic of Kazakhstan is an important element aimed to ensure the security of information resources and to protect citizens, organizations and state bodies from cyberthreats. Kazakhstan is the first country in Central Asia to adopt regulatory documents that govern the activities of the Internet community. In 1997, the President's message "Prosperity, security, and improvement of the well-being of all Kazakhstanis" presented Kazakhstan's development strategy until 2030. It states that the country's national security depends on information security (Message of the President of the Republic of Kazakhstan Nursultan Nazarbayev to the people of Kazakhstan..., 2007).

Therefore, some features of information security in Kazakhstan can be distinguished:

Legislative framework: The Republic of Kazakhstan established the Institute of Informatics and Management Problems (2022) and adopted such fundamental legislative acts as "On State Secrets" (Law of the Republic of Kazakhstan No. 349-I..., 1999), "The State Program for the Formation and Development of the National Information Infrastructure of the Republic of Kazakhstan for 2001-2003" (2001).

State bodies: The Information Security Committee under the Ministry of Digital Development, Innovation and Aerospace Industry (2022) are in charge of the information security of the Republic of Kazakhstan. The Information Security Committee is entrusted with the task of developing international cooperation and administrative and technical measures and implementing state policy in the field of cybersecurity, including market one. Kazakhstan has a National Information Security Centre (NISC), which is responsible for coordinating and monitoring information security in the country. The NISC is responsible for threat analysis, policy and strategy development and coordination of information security activities. Kazakhstan pays particular attention to cybersecurity and cyber-threats. Special centres for the detection and prevention of cyberattacks were established in the country. Apart from that, trainings are organized to improve the skills of specialists in the field of cybersecurity.

International cooperation: Kazakhstan actively cooperates with international partners in the field of information security, including the United Nations, OSCE and other organizations. This cooperation includes the exchange of information on cyber-threats, joint projects and programmes.

Education and awareness: In Kazakhstan, attention is paid to increasing public information literacy and awareness of information security. Educational programs and trainings for a wide audience and special courses for specialists in the field of information security are held.

So far, there are about 40 companies in Kazakhstan, 19 private security operations centers (SOCs), three computer emergency readiness teams (CERTs), seven private certified testing laboratories, eight higher education institutions, and 25 secondary education institutions dealing with cybersecurity issues.

Over the past few years, Kazakhstan has elaborated basic approaches to the development of cybersecurity in the country. One of these approaches is the "Cybershield of Kazakhstan" concept (2017). Its purpose is to determine the key directions of the state policy implementation in the field of IT and telecommunications, protect electronic information resources, increase digital literacy among the population and business, and ensure the safe use of information and communication technologies. A new version of the concept "Cybershield of Kazakhstan-2" will be adopted in the second half of 2022. Within the framework of its implementation until 2027, there will be the presentation of the principal directions for strengthening administrative responsibility for the leakage of personal data, the development of domestic software, the use of Kazakhstani social and media platforms, and the regulation of the activities of foreign ones. Moreover, this document will consider the challenges and cyber threats in the context of international experience and the views of domestic experts in the field of cybersecurity.

However, numerous legislative acts and orders in the field of cybersecurity have already entered into force. In addition, information security testing laboratories for malicious code research have been set up, a national information security coordination center, a private computer emergency readiness team (CERT), and seven security operations centers (SOCs) have been launched, and the number of grants in this field has been increased.

In order to improve the situation in the field of information security and personal data protection, the Ministry of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan raised the issue of assigning the Information Security Committee with the functions of protecting personal data, conducting audits and inspections of owners of information systems for personal data processing.

On June 21, 2021, President of the Republic of Kazakhstan Kassym-Jomart Tokayev signed a Decree “On approval of the National Security Strategy of the Republic of Kazakhstan for 2021-2025” (2021). The new National Security Strategy of the Republic of Kazakhstan was the sixth of its kind to be adopted at the time of independence. The Law “On National Security of the Republic of Kazakhstan” defines the Strategy as a strategic document for state development, which determines the main challenges and threats, strategic goals and target indicators, and objectives and result indicators in the field of national security. In addition, this Strategy is one of the elements of the national planning system and is developed in the context of the implementation of the Development Strategy of Kazakhstan by 2050.

Kazakhstan today is on a course for the formation and establishment of its mechanisms for information security protection. It is first necessary to do the following in order to develop the industry:

1. To design educational channels dedicated to digital communications and skills. There must be a balance between educational content and applied lessons and materials aimed at developing skills and potential employment.

2. To develop thematic event formats for exchange of views and participatory design. In such a way, extra-institutional mechanisms for young people and their dialogue with decision-makers will come into service at all levels.

3. To expand online and offline platforms for the participation of the target audience in social and economic activities, such as the promotion of internships and training opportunities through job shadowing, the development of mentoring programs, the improvement of vocational guidance and counseling in schools and universities, the expansion of opportunities for volunteering and summer programs.

4. To establish youth solidarity funds, including small grant programs, to promote countering violent extremism initiatives at the community, local, or grassroots levels.

5. To develop a mobile gaming industry aimed at education and awareness-raising on radicalization and its consequences.

4. Information security of Ukraine

Information security occupies a special place in the national security system of Ukraine. Ukraine is actively working on the development and implementation of strategic measures and policies aimed at ensuring information security and protection against cyber-threats. The provision of information security is one of the essential government functions in Ukraine since the country has experienced unusual information attacks from the Russian Federation shortly after the Revolution of Dignity. Ukraine has not focused its attention on information security for 20 years of its independence, and the result is annexed territories and misinformed minds of people in non-government-controlled areas.

Ukraine began to talk more or less actively about strategic communications in 2014 when Russia resorted to armed aggression. An important component of the latter was a disinformation campaign, when Russian propaganda called Ukraine a failed state, coming up with stories about “crucified boys” and other things. In such a way, the Kremlin tried to show the world that the “civil war” did not stop in Donbas, and Ukrainians and Russians “were one people”.

At the institutional level, numerous government bodies are in charge of the provision of particular areas of information security, namely, the Ministry of Information Policy, the National Council and the State Committee for Television and Radio Broadcasting of Ukraine, the National Commission for the State Regulation of Communications and Informatization, the Ministry of Foreign Affairs of Ukraine, the Ministry of Internal Affairs of Ukraine, the Security Service of Ukraine, and the State Service of Special Communications and Information Protection of Ukraine. Divisions for strategic communications have appeared in government structures and universities of Ukraine. In particular, it is a question of the Educational and Research Center of Strategic Communications in the sphere of National Security and Defense at the National Defense University of Ukraine named after Ivan Cherniakhovskyi and management of strategic communications of the Staff of the Commander-in-Chief of the Armed Forces of Ukraine.

The implementation of the state policy in this area is entrusted to the central executive body – the Ministry of Information Policy of Ukraine, which has been the main body responsible for national information security since 2015. Notably, one of the successes of the Ministry of Information Policy is the adoption of the Doctrine of Information Security of Ukraine (2017). The purpose of the Doctrine is to clarify the basis for the formation and implementation of state information policy primarily to counteract the destructive information influence of the Russian Federation in the context of its hybrid war.

The Cabinet of Ministers of Ukraine approved the Information Security Strategy (2021) on September 15, 2021. This Strategy is one of the numerous documents developed to implement the National Security Strategy of Ukraine. Its purpose is to establish conditions for ensuring the information security of Ukraine, aimed at

> "Daniel Rohder and Steven Schneider consider how the information security tools can be used to build trust and improve relationships between government, business, and citizens in a digital world."

protecting the vital interests of a citizen, society, and the state in countering internal and external threats. The Strategy also lays the groundwork for the protection of sovereignty and territorial integrity of Ukraine, support of social and political stability, national security, and guarantee for the rights and freedoms of every citizen. The implementation of the Strategy is planned for the period up to 2025.

The expected result of the implementation of the Strategy is a secure information space in Ukraine, which includes effective counteraction to an illegal content, promotion of an effective system of strategic communications, and enhancement of media culture and media literacy of the population. However, its relevant section provides only general definitions of the desired state in case of implementation of the Strategy. A more detailed description of the state of affairs in the field of information security or particular quantitative and qualitative indicators could better inform about the effectiveness of the implementation of this Strategy. The National Security and Defense Council can finalize the information security strategy before its approval by the President of Ukraine. In general, it is a framework document and does not provide an opportunity to assess the extent to which its implementation will affect the exercise of digital rights. It is necessary to consider the following nuances when developing an action plan and legislation for the implementation of the Strategy. Any legislative measures aimed at countering disinformation and restricting access to harmful content on the Internet may impose limitations on the right to freedom of expression only if they meet the requirements of legality and proportionality. The public authorities involved in the implementation of the Strategy should have a clear-cut distribution of powers, and their activities should be transparent. In particular, it is necessary to strictly define the body in charge of the implementation of the Strategy, who will analyze and report to the public on the effectiveness of the measures taken to implement it.

The Center for Strategic Communications and Information Security (2022) operates under the Ministry of Culture and Information Policy of Ukraine. The focus of the Center's work is the counteraction to external threats, integration of efforts of the state and public organizations in the fight against disinformation, prompt response to fakes, and promotion of Ukrainian narratives.

The key objectives of the Center are as follows:

- To develop strategic communications (counter-narratives of the Russian Federation, information campaigns, inclusion of Ukrainian narratives in the daily communication of the Government).
- To counter and build resilience to disinformation (a permanent notification of information attacks against Ukraine on the resources of the Center, in particular on the web-portal, FB-page, and Telegram channel).
- To raise awareness of hybrid threats (a design and training delivery for civil servants, representatives of communication units, in particular).
- To report hybrid aggression by Russia regularly at the international level, to develop mechanisms to counteract disinformation with the help of international partners.

In order to achieve this purpose, the Centre produces numerous information products that are as follows:

1. Center communication platforms (website and official social media pages).
2. Message box "The main positions of the information response. We explain complex things in simple words" (a daily analysis of the main events and the established theses for their explanation. Such theses are of avail to the daily work of politicians, civil servants, communicators of government bodies, journalists, and experts in other categories. For different audiences).
3. Daily Digest "How Russian Propaganda Works in Time of War".
4. Analytical digest, which is published on a daily basis and contains a description of the collected materials

about propaganda and narratives used in the media space of Russia.

5. A series of products under the general name *dovidka.info* (an updated directory "In case of emergency or war," website dovidka.info, and chatbots with the daily mailing of up-to-date tips and recommendations).

6. Training element for civil servants (Pieces of training dedicated to disinformation, fakes, and the basics of effective communication; short lectures and webinars on current issues, including fakes and their recognition in the network, hybrid warfare, and propaganda).

Ukraine is the first country to enshrine the concept of strategic communications in official acts – the Military Doctrine of Ukraine (Decree of the President of Ukraine No. 47/2017…, 2017), the Doctrine of Information Security of Ukraine (Huberskyi, 2004), and the Strategy of Information Security of Ukraine (2021).

The action plan for the implementation of the Strategy should provide clear indicators to measure the effectiveness of its implementation. There must be full rather than formal public involvement ensured to implement the Provisions of the Strategy and design an action plan. Since Ukraine is an orthodox country, and the church occupies a significant place in the lives of Ukrainians, pro-Russian activists continue to misinform people with the help of the church to this day; it complicates the implementation of the communications strategy.

The provision of territorial integrity and national security as the foundations of the national unity of Ukraine requires the highly effective implementation of the provisions of current legislation (legal rules) in the information activities of public servants. The above is possible only provided that methods and forms of public administration of the subjects of power are further improved, their legal culture and professional competence are high, and electronic governance in Ukraine further develops. It is necessary to systematize and algorithmically use mechanisms to ensure internal information security and form support for Ukraine in the societies of partner countries through information domination in its territory, effective repression of Russian information attacks, and the development of high-quality content for access to external information spaces.

Ukraine pays attention to improving information literacy and citizens' awareness of information security. Educational campaigns, seminars and trainings are conducted to raise awareness of cyber-threats, network security and correct behavior in the digital space. In general, Ukraine is actively developing and improving information security capabilities to protect its information resources, citizens and critical infrastructure from cyber-threats.

5. Information security policy in the EU

The Information Security Policy in the European Union is s based on the desire to provide a high level of information and data protection to support the security of EU citizens, enterprises and Member States. The EU has taken a wide range of measures and initiatives to strengthen information security at the regional level. The European Union pursues an active information security policy. In 2001, the European Commission presented the first document entitled "Network and Information Security: Proposal for European Policy Approach," which outlined a European approach to issues of information security. The document uses the term "network and information security," interpreted as the ability of a network or an information system to resist accidental events or malicious actions that pose a threat to the availability, authenticity, integrity and confidentiality of stored or transmitted data as well as related services offered via these networks and systems (Communication of European Commission: Network and Information Security: Proposal for European Policy Approach, 2001).

The document defines the following main directions of the European information security policy:

1. To increase users' awareness of possible threats when using communication networks. Priority activities in this area include public information and education campaigns, the promotion of best practices in the field of security, and the development of training courses on security issues.

2. To establish a European warning and information system. The main task of the EU countries is to design a confidential mechanism for attack notification for business entities and a user warning system that informs about the danger and gives advice on countering attacks. Following this purpose, Member States should revise the technical support and competence of national computer emergency response teams (CERTs) and enhance the cooperation between computer emergency response teams and similar structures in other countries.

3. To ensure technology support. Support for network and information security research takes priority. In order to achieve this purpose, the EU Framework Research Program should involve security issues, and the Member States are encouraged to promote the active use of variable encryption.

4. To support market-oriented standardization and certification. The existence of numerous competing standards and specifications in the field of information security is the main problem in the EU, which leads to market fragmentation and incompatible solutions. The proposed solvation to this problem implies the following: to revise the existing safety standards; develop compatible and safe goods and services; promote the use of certification and accreditation procedures in accordance with generally accepted European and international standards.

5. To provide legal support. The priority directions of the EU policy in the field of legal regulation of information security are the protection of personal data, telecommunication services, and cybercrime. They also involve the establishment of favorable conditions for the free circulation of encryption products and services by the Member States through the harmonization of administrative export procedures and the relaxation of export control.

6. To strengthen security at the state level. The issue of security is essential for the further development of e-governance. The main task of the state authorities is to promote the development of a safety culture. In this area, it is planned to introduce effective and compatible means of information security and encourage the Member States to use electronic signatures while providing public online services.

7. To develop international cooperation in the field of information security. The primary task of the EU is to reinforce the dialogue of the European Commission with international organizations and partners on the problem of network security and, in particular, the increased dependence on electronic networks.

The European Network and Information Security Agency (2022) was established on March 10, 2004. Its purpose is to strengthen the capabilities of the European community, Member States, and the business community to prevent and respond to information security-related issues. The main areas of the Agency's activity are as follows: provision of advisory and assistance services to the Commission and the Member States in the field of information security; data collection and analysis regarding security incidents in Europe and emerging risks; design of risk assessment and management techniques to improve the EU's response to information security threats; awareness raising and the promotion of cooperation between different actors in the field of information security by stimulating interaction between the public and private sectors. The Agency also assists the European Commission in preliminary technical work to update and improve the European legislation in the field of network and information security.

The EU pays significant attention to the issue of cybersecurity as a component of information security. The EU has been implementing Safer Internet Programmes since 1999. Each program lasts for 4-5 years. The Safer Internet Programme for 2009-2013 presupposed numerous measures to combat malicious content and dangerous behavior on the Internet (Safer Internet Programme, 1999). The main objectives of the Programme are to raise public awareness, provide the public with a network of contact points for reporting illegal and harmful content and behavior, promote self-regulatory initiatives in this area and involve children in designing a safer online environment, and develop a knowledge base on new trends in online technologies and their consequences for children's lives. Key aspects of information security policy in the EU are as follows:

Legislation and regulation: The EU develops and adopts regulations aimed at ensuring information security. For example, the General Data Protection Regulation (GDPR) establishes rules for the processing and protection of personal data in the EU.

Cooperation and coordination: the EU supports cooperation and coordination among member States in the field of information security. This includes sharing information on cyber-threats, general readiness exercises and response mechanisms to cyber-attacks.

Cybersecurity and critical infrastructure protection: The EU is developing measures and standards to protect critical information infrastructure, such as energy systems, transportation networks, and financial institutions from cyber threats.

Research and innovation: the EU supports research and development in the field of information security. Projects and initiatives are funded to develop new technologies and solutions in the field of cybersecurity.

Building the information culture: The EU aims to increase information literacy and awareness among citizens, businesses and authorities. Educational programs and information campaigns were being implemented to raise awareness of threats and promote safe behavior in digital space.

International cooperation: the EU actively cooperates with international partners and organizations in the field of information security. Partnerships are being established to share information, coordinate responses to cyberthreats and develop international standards and norms.

The adoption of the European Commission Communication "A Strategy for a Secure Information Society: Dialogue, Partnership, and Empowerment" (2006) was significant progress in the European policy development in this area. The Strategy provides an overview of the current state of security threats to the information society and identifies additional security measures. In 2016, the EU agreed on pan-European principles of information security. The European Parliament approved a new directive that listed the sectors of the economy (energy, transport, banking services) that would have to guarantee their ability to prevent cyber-attacks Moreover, companies are obliged to inform the national authorities in case of a serious information security incident. Digital service providers such as Amazon or Google need to facilitate information sharing (Directive on Security of Network and Information Systems, 2016).

The EU needs to implement numerous measures in order to respond adequately to existing cybersecurity challenges:

1. To ensure an adequate level of training at all levels. The Member States should identify basic capabilities for national computer emergency response teams and security incident response systems. This also implies strengthening cooperation between the public and private sectors and establishing a European forum for information exchange between the Member States.

2. To establish a European cyber-attack early warning system.

3. To strengthen security mechanisms for the EU's critical information infrastructure, develop national emergency response plans and institutional relations, conduct a pan-European training on Internet security incidents, and enhance cooperation between national computer emergency response teams.

4. To develop European guidelines on Internet sustainability and stability and their promotion in the international arena.

5. To determine the criteria for identifying the critical infrastructure of Europe for the information and communication technology sector.

Both public authorities and non-governmental organizations are to implement political priorities defined by the governing bodies of the European Union in the field of information security at the national level.

The approaches developed in the European Union for ensuring information security reflect the agreed freedom of the EU Member States and institutions and represent European framework standards in this area. The above countries can successfully apply these standards in case of their adaptation to the features of state legal systems and socio-cultural specifics.

The EU's information security policy is dynamic and evolving to meet the changing cyber environment and protect the interests of citizens and organizations in the EU.

6. Recommendations for strategic communications development

The Communications Strategy for Information Security is indeed an important tool in countering hybrid warfare. Hybrid warfare is a combination of different methods, including information operations, cyberattacks, and manipulation of public opinion, to achieve political and military goals. The world experience shows that an effective communication strategy for information security should include the following components:

1. Vulnerability analysis and assessment: It is important to analyse information vulnerabilities and identify potential threats. This will allow the development of appropriate measures to protect information.

2. Crisis management: Crisis management plans need to be developed that include measures to detect, respond to and recover from information attacks. Quick and adequate response to incidents will help minimize their consequences.

3. Public communication: It is important to establish an open and confidential dialogue with the public. This can be achieved through information campaigns, press conferences, Internet resources and social media. Governmental and non-governmental organizations should provide reliable information on the current situation, threats and measures taken.

4. International cooperation: Hybrid warfare often has a cross-border character, so it is important to develop international cooperation in the field of information security. Exchange of experience, coordination of measures and joint efforts make it possible to deal more effectively with hybrid threats.

5. Integrated approach: The communication strategy should be part of an integrated approach to information security. It should interact with technical protection measures, training of personnel, legislation and other aspects of information security.

The communication strategy should focus on the system of target audience parameters, including the cultural awareness of current and historical values, norms, and beliefs reflected in various social structures or their effect on the motives, intentions, and behavior of the target audience (Plotnikova, 2011). The communication strategy should also consider the existing psychological situation – the emotional state, mentality, and other behavioral motivations of the target audience. These behavioral motivations are based mainly on national, political, social, economic, and psychological features, but circumstances and events can also influence them.

The approach to the strategy formation should do the following:

- To be adaptive and flexible, i.e., consider the capabilities and needs of all participants in communication.
- To consider possible risks for effective decision-making on the loss balance due to these risks and benefits.
- To be based on analysis of the information environment, in-depth assessment of the situation and forecasting for effective decision-making.

- To be focused on communication and interaction among all StratCom actors to ensure mutual understanding and unity of purpose and action.

It is necessary to calculate the effectiveness of the target audience, i.e., their ability to implement the desired reaction or behavior of their own or others as a result of the implementation of the strategy. The strategy should be flexible, in other words, easily adaptable to changing requirements. These requirements can be predictable and unpredictable and affect, for example, the configuration, application, placement, or use of certain information materials. The actions envisaged by the strategy must be synchronized, i.e., coordinated in time and space.

Innovation is not a thing to be afraid of. Innovation is often perceived as a threat to existing potential and investments. Since innovation is always subject to doubts, it often means preparation for possible conflicts (Joint Concept Note 1/17 Future Force Concept, 2017). In recent years, numerous events that demonstrate it is possible to lose the target audience's trust or strengthen it with effective strategic communications just in a few hours have taken place in the world.

Strategic communications are an effective tool for overcoming hybrid threats. Its effectiveness is determined by the system-provided implementation of the following algorithm of actions:

1. Analysis – monitoring – assessment of the information environment and hybrid threats. The StratCom system development implies preliminary research and analytical activities, which are solved in the "analysis – monitoring – assessment" system. This involves processing the structured data obtained from various sources in order to identify objects, connections, and ways of behavior in the process of conducting influential events. At this stage, political, military, and civilian authorities need to consult with civil society experts to coordinate positions and develop recommendations for the StratCom introduction.

2. Development of a strategic concept. A strategic concept means "a flexible course of actions adopted as a result of the strategic situation assessment to form the structure and content of military, diplomatic, economic, psychological, and other relevant measures of the StratCom" (NATO Glossary of Terms and Definitions (English and French). North Atlantic Treaty Organization NATO Standardization Office (NSO), 2014).

3. Development of a nationwide strategic narrative, its systematic broadcasting to various target audiences via all StratCom components, including public relations, public diplomacy, civil-military cooperation, information supply, and software. The following actions should accompany this process:

    - To develop institutional (operational/tactical) narratives supporting the strategic one and detailing it for a specific target audience.

    - To maintain a strategic narrative through strategic content broadcast via different communication channels, taking into account the portrait of a particular target audience.

    - To develop coordination mechanisms between all actors of strategic communications. This involves identifying the target audience, namely recipients of narratives and messages, and designing an algorithm for communicating the main messages to representatives of the SDB of different ranks and for all target audiences on the components of StratCom.

4. Determination of the effectiveness of strategic communication activities that include indicators reflecting an increase or decrease in particular activities of the target audience. Indicators help to analyze and demonstrate the effectiveness of the activities according to StratCom. After the effectiveness is measured, adjustments to the strategic concept and its implementation plan are possible.

5. Consider context and culture: When designing communication strategies and messages, consider the context and culture of your audience. Adapt your language, images, and symbols to be understandable and relevant to your audience.

6. Pay attention to two-way communication: Do not forget the importance of two-way communication. Set up feedback mechanisms, conduct surveys and research to understand the opinions and needs of your audience. This will help you better customize your communication strategies and improve interaction with the audience.

7. Educate communication professionals: Invest in the learning and development of communication professionals. Confident and competent communicators will be able to effectively represent your organization and achieve communication goals.

8. Measure and evaluate results: Set metrics and a system to evaluate the effectiveness of your communication efforts. Measuring results will allow to determine the success of your strategies and make the necessary adjustments.

In order to achieve effective communication, it is necessary to build models and forms of cooperation between stakeholders and between them and other potential partners. By expanding the network of possible alliances, we increase the power of influence and the spread of favorable messages. It is important to remember that strategic communication is an ongoing process and that it must be flexible and adaptable to the changing circumstances and needs of your audience.

7. Conclusions

Targeted manipulation of public opinion with brainwashing technologies is one of the most dangerous manifestations of hybrid war, which the aggressor state implements against the opponent. Information security is a characteristic of a stable, sustainable public administration system, which retains its vital components when exposed to internal and external threats. In other words, information security is responsible for protecting the interests of citizens and the state in the information environment from various real or virtual threats. It is important to note that information security policies vary from country to country depending on their needs, characteristics and level of development.

After the Revolution of Dignity, Ukraine involuntarily became a participant in the hybrid war, which forced it to think about information security and communication with the occupied areas in the shortest possible time. The result is a competent, albeit belated, communication strategy for information security.

The concept of information security for Kazakhstan is revealed through the strategy of its existence as a sovereign and stable state, as well as the development and implementation of a purposeful systemic and balanced policy of protecting national interests from external and internal information threats.

The European Union attaches great importance to information security since it considers it essential for the successful development of the information society. The cross-border nature of information threats necessitates the implementation of a set of measures at the pan-European level, the harmonization of national systems for countering these threats, and the development of cooperation between national and European bodies in the European Union.

The EU specialized institutions (Europol, Eurojust, the ENISA agency) for coordination and information and analytical support of the activities of national law enforcement and other bodies complement the activities of the central EU institutions (the European Commission, the European Parliament, and the EU Council) for development of a strategy and strengthening the legal framework for countering threats to information security. The activity of the EU institutions and bodies in the field of information security is most pronounced in the

former first pillar (European Community) and third pillar (cooperation between police and criminal courts). However, no systemic work is observed in the second pillar (common foreign and security policy).

Public-private partnerships in this area attract significant attention, and the same is for the involvement of civil society institutions and the corporate sector in information security activities at the national and pan-European levels.

8. References

Australian Government. (2016). *Australia's cyber security strategy. Enabling innovation, growth & prosperity.* https://www.homeaffairs.gov.au/cyber-security-subsite/files/PMC-Cyber-Strategy.pdf

Belkin, L., Iurynets, Ju., Sopilko, I., & Belkin, M. (2022). Culture and the use of information understanding in the field of national security (a case study of Ukraine). *Journal of International Legal Communication, 5*(2), 36-58. https://doi.org/10.32612/uw.27201643.2022.5.pp.36-58

Bjola, C., & Holmes, M. (2015). *Digital Diplomacy: Theory and Practice*. Routledge.

Bogush, V. (2005). *Information security of the state*. Kyiv: MK-Press.

Cavelty, M. D. (2008). *Securing the Homeland: Critical Infrastructure, Risk, and (In)Security*. Routledge.

Center for Strategic Communications. (2022). https://spravdi.gov.ua/pro-nas/

Clarke, R. A, & Knake, R. (2011). *Cyber War: The Next Threat to National Security and What to Do About It*. Ecco.

Decree of the President of the Republic of Kazakhstan. (2021). *On approval of the National Security Strategy of the Republic of Kazakhstan for 2021-2025*. https://acortar.link/zNFD2C

Decree of the President of the Republic of Kazakhstan No 573 (2001). *State program for the formation and development of the national information infrastructure of the Republic of Kazakhstan for 2001-2003*. https://adilet.zan.kz/rus/docs/U010000573_

Decree of the President of Ukraine No. 47/2017. (2017). *On the Doctrine of Information Security of Ukraine*. http://www. president.gov.ua/documents/472017-21374

Decree of the President of Ukraine No. 685/2021. (2021). *Information security strategy of Ukraine*. https://zakon.rada.gov.ua/laws/show/685/2021#Text

Decree of the President of Ukraine No. 685/2021. (2021). *On the decision of the National Security and Defense Council of Ukraine from 2021 "On Information Security Strategy"*. https://acortar.link/j6CHnH

Directive on Security of Network and Information Systems. (2016). E*urope agrees cyber threat strategy, plans to help fund more startups*. https://acortar.link/XG7Fqx

Huberskyi, L. V. (2004). *Ukrainian diplomatic encyclopedia*. Kyiv: Knowledge of Ukraine.

Information Security Committee under the Ministry of Digital Development, Innovation and Aerospace. (2022). https://www.gov.kz/memleket/entities/infsecurity?lang=ru

Institute for Informatics and Control Problems. (2022). https://iict.kz/ru/istoria-instityta/

Isikoff, M., & Corn, D. (2018). *Russian Roulette: The Inside Story of Putin's War on America and the Election of Donald Trump*. Twelve.

Kalyuzhny, R. (2000). The issue of the concept of reforming information legislation of Ukraine. *Collection Legal, normative and metrological support of the information protection system in Ukraine*, 17-21.

Kordunian, I. (2022). Establishment of the institute of mediation in Ukraine at the legislative level. *Journal of International Legal Communication, 5*(2), 108-116. https://doi.org/10.32612/uw.27201643.2022.5.pp.108-116

Kormych, B. A. (2004). *Information security: organizational and legal foundations*. Kyiv: Condor.

Law of Republic of Kazakhstan No 349-I (1999). *About state secrets*. https://online.zakon.kz/Document/?doc_id=1012633

Lipkan, V.A. (2006). *Information security of Ukraine in the conditions of European integration*. Kyiv: KNT.

MCM-0085-2010 STRATCOM. NATO. (2010). *Military Concept for Strategic Communications*. https://info.publicintelligence.net/NATO-STRATCOM-Concept.pdf.

Message of the President of the Republic of Kazakhstan N.Nazarbayev to the people of Kazakhstan (Part III). (2007). *Strategy "Kazakhstan-2030" at the New Stage of Development of Kazakhstan. 30 most important directions of our domestic and foreign policy*. https://online.zakon.kz/Document/?doc_id=30090778&pos=2;-106#pos=2;-106

NATO Glossary of Terms and Definitions. (2014). *North Atlantic Treaty Organization NATO Standardization Office (NSO)*. wcnjk.wp.mil.pl/plik/file/N_20130808_AAP6EN.pdf

Oxford English Dictionary. (2022). *Post-truth.* http://www.oed.com

Plotnikova, S. (2011). *Technologization of discourse in modern society*. Iruktsk: IGLU.

Safer Internet Programme. (1999). http://ec.europa.eu/information_society/activities/sip/policy/programme/current_prog/index_en.htm

Schwartau, W. (1996). *Information Warfare*. Thunder's Mouth Press.

Sopilko, I. (2022). Cyber threat intelligence as a new phenomenon: legal aspect. *Journal of International Legal Communication, 4*(1), 8-18. https://doi.org/10.32612/uw.27201643.2022.1.pp.8-18

Cyber Shield of Kazakhstan. (2017). https://adilet.zan.kz/rus/docs/P1700000407

The European Network and Information Security Agency. (2022). http://www.enisa.europa.eu/

Voitovy, R. (2019). *Information security: approaches to defining the concept*. https://n9.cl/a1w4b

Zharkov, Y. M., & Besedina, L. M. (2009). Directions of external informational and psychological influence on Ukraine. *Collection of Scientific Works of the Military Institute of T. Shevchenko National University of Kyiv*. http//www.nbuv.gov.ua/portal/natural/znpviknu/2009-19/vip19-21.pdf

9. Related articles

Agudelo González, L. E., Marta-Lazo, C., & Aguaded, I. (2022). Competencias digitales en el Currículo de Periodismo: Análisis de caso de una universidad Centroamericana. *Vivat Academia. Revista de Comunicación*, 155, 297-316. https://doi.org/10.15178/va.2022.155.e1393

Aladro Vico, E. (2020). Comunicación sostenible y sociedad 2.0: particularidades en una relación de tres décadas. *Revista de Comunicación de la SEECI*, 53, 37-51. https://doi.org/10.15198/seeci.2020.53.37-51

Carrera, P., Blanco-Ruiz, M., & Sainz-de-Baranda Andújar, C. (2020). Consumo mediático entre adolescentes. Nuevos medios y viejos relatos en el entorno transmedia. *Historia y Comunicación Social, 25*(2), 563-574. https://doi.org/10.5209/hics.72285

Conde del Río, M. A. (2021). Estructura mediática de Tiktok: estudio de caso de la red social de los más jóvenes. *Revista de Ciencias de la Comunicación e Información*, 26, 59-77. https://doi.org/10.35742/rcci.2021.26.e126

López-Borrull, A. (2022). Invasión rusa en Ucrania: análisis desinformativo de la primera semana de conflicto. *COMeIN*, 119. https://doi.org/10.7238/issn.2014-2226

AUTHORS' CONTRIBUTIONS, FINANCING AND ACKNOWLEDGMENTS

Author contributions: Authors' contributions are equal.

Financing: The authors did not receive support from any organization for the submitted work. No funds, grants, or other support was received.

Conflicts of Interest: The authors declare they have no financial and competing interests.

AUTHORS:

Arailym Nussipova
Doctor en Ciencias Sociales. Departamento de Kazakh-American University International Educational Corporation 050043, 28 Ryskulbekova Str., Almaty, República de Kazajstán.
arailym_nussipova@sci-academy.cc

Orcid ID: https://orcid.org/0000-0002-4112-1971
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57693920100

Gulzhan Khussainova
PhD in Philosophy and Associate Professor. Department of Social and Political Disciplines K. Zhubanov Aktobe Regional University 030000, 34 A.Moldagulova Ave., Aktobe, Republic of Kazakhstan.
gulzhan_khussainova@un-nyc.net

Orcid ID: https://orcid.org/0000-0002-8893-1517

Raushangul Kabilova
PhD in Philosophy and Associate Professor. Department of Kazakh-American University International Educational Corporation 050043, 28 Ryskulbekova Str., Almaty, Republic of Kazakhstan.
raushangul_kabilova@sci-academy.cc

Orcid ID: https://orcid.org/0000-0001-8017-4868

Esenzhol Aliyarov
Full Doctor of Political Science and Professor. Association of Political Studies 500500, 68/74 Abay Ave., Almaty, Republic of Kazakhstan.
esenzhol_aliyarov@pltch-sci.com

Orcid ID: https://orcid.org/0000-0002-4173-7100
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57579013900

Botakoz Nuralina
Master of humanitarian science and Assistant professor. Department of Kazakh-American University International Educational Corporation 050043, 28 Ryskulbekova Str., Almaty, Republic of Kazakhstan.
botakoz_nuralina@sci-academy.cc

Orcid ID: https://orcid.org/0000-0002-7634-522X