ppi 201502ZU4645
Publicación científica en formato digital
ISSN-Versión Impresa 0798-1406 / ISSN-Versión on line 2542-3185
Depósito legal pp 197402ZU34

CUESTIONES POLÍTICAS

Instituto de Estudios Políticos y Derecho Público "Dr. Humberto J. La Roche"
de la Facultad de Ciencias Jurídicas y Políticas de la Universidad del Zulia
Maracaibo, Venezuela

Vol.40 | Nº 74
2022

Cuestiones Políticas Vol. 40, N° 74 (2022), 741-763
IEPDP-Facultad de Ciencias Jurídicas y Políticas - LUZ

Improved Planning of Information Policy in the Cyber Security Sphere under Conditions of Hybrid Threats

DOI: https://doi.org/10.46398/cuestpol.4074.41

Viacheslav Dziundziuk *
Olena Krutii **
Roman Sobol ***
Tetiana Kotukova ****
Oleksandr Kotukov *****

Abstract

The study aimed to consider the current state of planning information policy in the field of cybersecurity under intensified hybrid threats, using the methods of comparison and observation. The study conducted showed that in the face of intensified hybrid threats, states must develop common approaches to implement state information policy and ensure information cybersecurity. In the face of Russia's hidden and direct aggression, governments should develop an effective system for implementing national information policies to ensure information security and introduce new state structures and mechanisms for timely detection and neutralization of threats to national interests in the sphere of information security. It concludes on the need to counter the destructive behavior of states using hybrid threats at the national and supranational levels and explains the low level of information protection in individual states and international institutions. The European Union and NATO can play a key supporting role and offer support where national responses to cybersecurity threats have proved insufficient.

Keywords: information threats; hybrid threat; state cybersecurity; disinformation; information policy.

* Doctor of Science in Public Administration, Professor, Department of Public Policy, Institute of Public Administration, V. N. Karazin Kharkiv National University, 61022, Kharkiv, Ukraine. ORCID ID: https://orcid.org/0000-0003-0622-2600

** Doctor of Science in Public Administration, Professor, Department of Public Policy, Institute of Public Administration, V. N. Karazin Kharkiv National University, 61022, Kharkiv, Ukraine. ORCID ID: https://orcid.org/0000-0002-5180-2842

*** Candidate of Sciences in Public Administration, Associate Professor, Department of Public Policy, Institute of Public Administration, V. N. Karazin Kharkiv National University, 61022, Kharkiv, Ukraine. ORCID ID: https://orcid.org/0000-0002-3176-3807

**** Candidate of Sciences in Public Administration, Associate Professor, Department of Public Policy, Institute of Public Administration, V. N. Karazin Kharkiv National University, 61022, Kharkiv, Ukraine. ORCID ID: https://orcid.org/0000-0001-8332-0330

***** Candidate of Sciences in Sociology, Associate Professor, Department of Public Policy, Institute of Public Administration, V. N. Karazin Kharkiv National University, 61022, Kharkiv, Ukraine. ORCID ID: https://orcid.org/0000-0003-2494-5298

Recibido el 15/07/22 Aceptado el 01/09/22

Mejora de la Planificación de la Política de Información en el Ámbito de la Ciberseguridad en Condiciones de Amenazas Híbridas

Resumen

El estudio tuvo como objetivo considerar el estado actual de la política de información de planificación en el ámbito de la seguridad cibernética bajo amenazas híbridas intensificadas, utilizando los métodos de comparación y observación. El estudio realizado mostró que, ante la intensificación de las amenazas híbridas, los Estados deben desarrollar enfoques comunes para implementar la política de información estatal y garantizar la ciberseguridad de la información. Frente a la agresión oculta y directa de Rusia, los gobiernos deben desarrollar un sistema efectivo para implementar políticas nacionales de información para garantizar la seguridad de la información e introducir nuevas estructuras y mecanismos estatales para la detección y neutralización oportunas de amenazas a los intereses nacionales en la esfera de la seguridad de la información. Se concluye sobre la necesidad de contrarrestar el comportamiento destructivo de los Estados que utilizan amenazas híbridas a nivel nacional y supranacional y se explica el bajo nivel de protección de la información en los Estados individuales y las instituciones internacionales. La Unión Europea y la OTAN pueden desempeñar un papel clave de apoyo y ofrecer soporte cuando las respuestas nacionales a las amenazas a la ciberseguridad hayan resultado insuficientes.

Palabras clave: amenazas de información; amenaza híbrida; ciberseguridad estatal; desinformación; política de información.

Introduction

Information can be defined as statistical and qualitative data and as beliefs that motivate professionals and mobilize the public (Maor, 2020). In the conditions of the development of innovative technologies, information can be considered a strategic national resource due to its increasing role in the national security system (Hlushko *et al.*, 2022). Information policy provides a set of principles that guide decision-making. The use of modern information resources requires a broad set of information policies.

At the state level, the top priority is the development of information policy, comprising the laws, regulations and doctrinal positions, as well as other decisions and practices that affect society as a whole, including the creation, processing, flows, access and use of information. Information policy includes such issues as net neutrality, filtering, intellectual property,

e-government and major social problems arising from the convergence of policies – levels of access and availability of infrastructure, social support of digital literacy, and digital integration of different population groups.

Digital technological developments and their growing interconnection with changes in social relations have allowed some states to challenge unfriendly countries using so-called "hybrid threats" – coordinated and synchronized actions, that specifically target the vulnerabilities of states and institutions through various online platforms (Dragos *et al*., 2020). This method of warfare entails the use of a wide range of well-designed tools that remain below the thresholds of detection, attribution and retaliation (Balcaen *et al*., 2022). Disinformation campaigns result in undermining vulnerable places of democracy, such as freedom of speech, and freedom of the media, exacerbating existing ethnic, religious, political or economic differences, which leads to decreased social cohesion (Wigell, 2019). Countries around the world have also faced a flurry of disinformation about COVID-19, which puts human lives at risk, raising doubts about the safety of approved vaccines and the reliability of imposed restrictions (Luo *et al*., 2021).

Resilience – the ability of states and societies to deter, resist, and overcome the impact of external interference – is needed to seriously confront hybrid threats in cyberspace, resulting in a demonstration of institutional capacity, good governance, and social cohesion (Bērziņa Čerenkova *et al*., 2019).

Countries differ in their approaches to countering hybrid threats in terms of the security organization and the scale of measures taken to deter the enemy's activities. At the same time, countries detect and respond to hybrid attacks in a similar way, which can be explained by the nature of hybrid threats (Wijnja, 2022).

National governments are developing the necessary information policy tools used in cybersecurity to counter hybrid threats, in the first place – means of communication with citizens and the possibilities of responding to cyber incidents and countering hybrid threats (Kalniete and Pildegovičs, 2021). Increasing user awareness allows us to avoid or neutralize undesirable consequences of information intervention that may occur during the digital transformation of the system (Taherdoost *et al*., 2021).

In modern conditions, Ukraine is the object of constant informational and psychological influence due to its geopolitical position and political and economic interest on the part of a large number of states. Ukraine is in a state of war, characterized not only by aggressive military attacks but also by the use of modern information technologies for hybridizing established rules of war (Veselova, 2021). In this context, the problem of ensuring the information security of national interests by improving approaches

to planning information policy in the field of cyber security is becoming increasingly important (Bondar and Rakutina, 2019).

Thus, given the above, the study aims to consider the current state of planning the information policy in the field of cyber security under hybrid threats. The research objectives are 1) to identify the main ways of improving information policy planning in the field of cyber security under conditions of hybrid threats in the case of Ukraine; 2) to reveal the current state of planning information policy mechanisms in the field of cyber security in the European Union and NATO in the context of helping Ukraine in the fight against hybrid threats.

1. Literature Review

The major toolkit and basis for the article was Howlett's (2019) work, dedicated to some significant and procedural tools of information policy in the era of globalization and innovative technologies, principles and methods, necessary for their implementation. The researcher evaluated the advantages, and disadvantages and provided a rationale for the use of specific information tools, revealed several problems and proposed recommendation solutions to them. The authors' position on the research topic was influenced by Maor's (2020) comprehensive analysis of the theoretical and legal foundations of policy design, the consequences of suboptimal plans, and the role of information quality in policy development.

In turn, Bondar and Rakutina (2019) defined the role of information security in information policy and determined possible prospects for optimizing the implementation of information policy and information security. The study took into account Wijnja's (2022) research on the specificity of individual countries and international cooperation on the liability for the actual use of counter-hybrid measures.

Special attention should be paid to the scientific work by Taherdoost and others (2021) on the systematization of scientific approaches to the concepts of "cyber security" and "information security" and the article by Zvezdova and Vakalyuk (2022) on the cyber security problem, challenges and dangers of high-tech cybercrime and cyber terrorism in modern hybrid warfare. Wigell (2019), Nilsson and others (2021) emphasized the need to develop a comprehensive approach to detecting, analysing and countering hybrid threats.

Kalniete and Pildegovičs (2021) stressed the need to intensify cooperation between the EU, NATO and the Eastern Partnership countries for further progress in cooperation against hybrid threats. Ratsyborinska (2022) traced the transformation of an innovative approach to the information policy

planning processes in the field of cyber security at the supranational level and its characteristics: innovativeness (novelty), objectivity, subjectivity, dedication, demand, implementation in practice, efficiency.

Multiple studies on this problem confirm the fact that special attention should be paid to the improvement of planning information policy in the cyber security sphere in light of hybrid threats. Therefore, it is necessary to conduct a study based on the new criteria of scientific research.

2. Methods

The research design was structured (Figure 1) given the multidimensional nature of the chosen research topic and the rapid dynamics of empirical material in the context of geopolitical transformations. The study is based on comparative research of different counties' positive experiences in the field of cyber security and on the grouping of the data obtained.

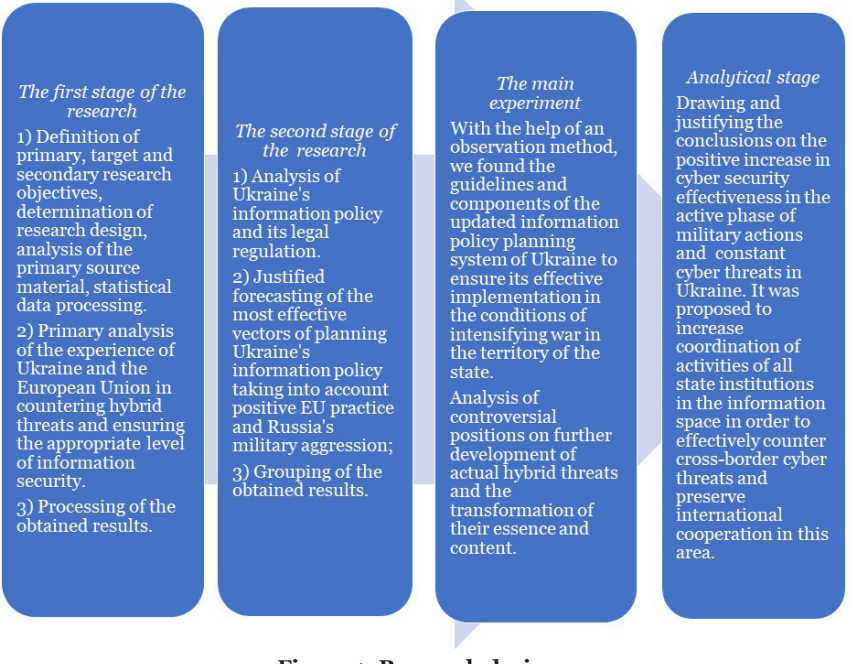

Figure 1: Research design

The main method of research is the method of observation, which allowed to achieve the aim and research objectives and identify the main vectors of improving information policy in the cyber security sphere of Ukraine in the context of modern challenges and draw attention to the expediency of improving coordination of activities of all state institutions in the information space.

The comparison method allowed us to judiciously compare the key statistical indicators of the implementation of the state's information policy and propose conceptual changes based on the most effective EU practices and new hybrid threats. The expediency of adopting EU practices into the legal field of Ukraine as soon as possible, which would also correspond to the declared postulates of future EU membership, was substantiated by this method.

The empirical content of information policy planning processes was based on the historical-genetic method, which allowed to describe the essential characteristics of information policy in the cyber security sphere, to uncover causal relationships in the development of hybrid threats and further transformations of state planning for effective protection, as well as in the organization of the state bodies activities regarding the prevention and protection of the population from disinformation.

In addition, an empirical basis for further evaluation of activities of state bodies and fiscal decentralization was created on the example of the state's development and indicators of its information security.

The historical-comparative method was used to determine the essential characteristics of government participation in the implementation of information policy and cyber security programs at different stages and to find positive features and critical disagreements in the implementation of effective information policy planning during different periods of statehood.

The statistical method was used to analyse the dynamics of implementation of cyber security programs at the national and supranational (the EU) levels, as well as to study a significant array of data on the actions of Ukraine and the EU.

A large amount of data was carefully analysed in the research, among which forty-three sources were cited within the text of the article.

3. Results

Information policy is used to denote political initiatives, that promote the use of tools and concepts related to the global information society, to realize their potential in achieving national, social and economic development

goals. The process of choosing the most effective and profitable options is the main way to make the necessary changes in creating reliable mechanisms for effective development of information policy, information planning and information management.

The information policy is aimed at the development of mechanisms that would promote compliance with reliability and availability of information, privacy, intellectual property rights, and storage of archival copies of materials. Its main areas are shown in Figure 2.

Planning of information policy is necessary to transform appropriate tactics into a set of actions. Approaches to strategic planning are distinguished by the following parameters: objectives, formalities, time period, completeness, organizational, inter-organizational and/or geographical focus, emphasis on data and analysis, degree of participation, place of decision-making, and links with implementation. In this context, it is necessary to identify and acknowledge the problems, to further develop, implement, and evaluate information policy.

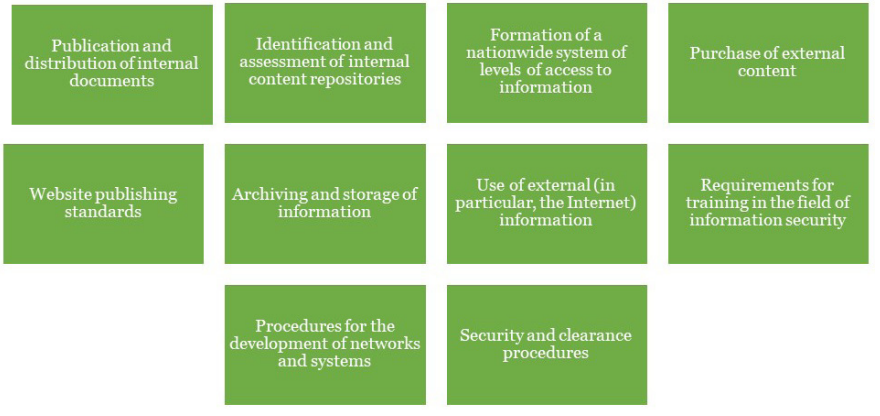

Figure 2: The main spheres of influence of information policy (compiled by the authors).

Information policy includes infrastructural, vertical, and horizontal levels. The infrastructural level deals with the development of the national (or in recent years regional) infrastructure, necessary to support the information society. As a rule, telecommunications policies are reviewed first, then the focus is given to separate policies. Vertical information policy involves such sectoral policies as education, tourism, production, and health care.

Horizontal information policy affects broad aspects of society, for example, policies on the freedom of information, tariff and pricing, and the use of information and communication technologies by the government within the country and in its relations with citizens, businesses, workers, and academia.

The target audience should be provided with truthful and convincing information based on national priorities, which leads to the great importance of the development of specialized scientific institutions, analytical centres, and mass media, which contain many information resources. Their primary task is to reflect the interests of citizens and state priorities.

The development of information policy in the cyber security sphere is influenced by the fact that hybrid threats in the information field are becoming more frequent and sophisticated and combine military and non-military, as well as covert and overt means, including disinformation, propaganda, cyber-attacks, special informational and psychological influence, economic pressure, the deployment of irregular armed formations and conventional armies.

Hybrid action is ambiguous, as hybrid actors blur the lines of international policies and operate at the intersections between external and internal, legal and illegal, peace and war. Each action has its algorithm, forms and methods of implementation. For example, the methods of external information aggression of special information operations are based on disinformation, diversification of public opinion, psychological pressure, and the spread of rumours.

The subjects of information security are directly the state, individual citizens, groups, and associations, which fulfil special functions for ensuring information security, given to them by law. The object of information security should be considered the psyche of a person, his/her consciousness, and even the consciousness of the masses, information systems for various purposes.

Objects of cyber protection include all types of communication systems, including relevant systems that are used for public inquiries and government electronic services and management. A special place is given to the objects of critical information infrastructure. A set of measures within various information protection regimes is of particular importance in today's reality (Figure 3).

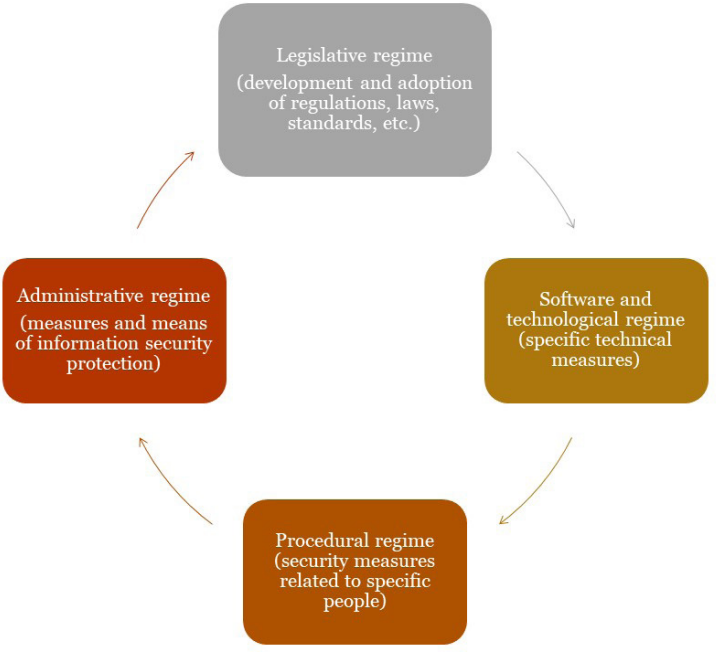

Figure 3: Measures of the main regimes of information protection (compiled by authors).

According to forecasts, the global information security market will reach 366.1 billion dollars by 2028 (Varonis, 2022). Information systems in cyberspace comprise all information infrastructures accessible through the Internet, including its largest and long-established segment web 2 with its social networks and platforms.

The communication network also includes a segment of mobile applications web 3 (on smartphones, tablets, and other similar devices); payment processing networks such as Paypal, SWIFT, Bitcoin and others; onboard processors for various objects of industrial and household infrastructure. Cyber-attacks can disrupt essential services and endanger the lives and safety of ordinary citizens.

They can be committed by organizations or private individuals who express their disagreement with the country's policy and promote their political agenda. Cyber actors can compromise information technology (IT) networks; develop mechanisms to support long-term permanent access to IT networks; withdraw sensitive data from IT networks and operational technologies; disrupt critical industrial control systems by installing destructive malware.

Cyber-attacks occur due to the use of unlicensed software and anti-virus software by state organizations and a low level of security of internal information and communication networks at critical infrastructure objects. Cyber fatigue or apathy towards proactive defence against cyber-attacks affects up to 42% of companies in all countries (Cisco Cybersecurity Report, 2020).

Personal attacks include negative and hurtful comments on victims' social media pages, usually anonymously or using pseudonyms. An example of hybrid threats to citizens in cyberspace can be the activities of troll farms, that is the creation of space in social networks to promote trolling as a kind of serious criticism. Besides, there are controversial, instructive posts to form the necessary opinion.

The provocative nature of the post is fuelled by anonymous and pseudo-anonymous comments, made by digital attackers. Meta trolling in videos is used by content creators (often acting as micro-influencers) to criticize popular political issues and is usually politically motivated and targeted at government and military websites. Placing or reposting memes on various forums disrupts the conversation, inflames emotions, and makes imperceptible but obvious changes to the information space.

In modern conditions, special attention is drawn to the information policy of Ukraine, which strongly resists Russian cyberattacks. Russian information operations are focused on encouraging and supporting separatist armed forces that create chaos and territorial disintegration; increasing polarization between elites and society to provoke a value crisis with a further process of reorientation towards Russian values; demoralizing the military and undermining their commitment; undermining socio-economic stability; provoking a socio-political crisis; intensification of psychological warfare to demoralize the armed forces and the population to break their determination to fight; inciting mass panic and undermining confidence in the most important state institutions; false information about political leaders who do not share Russia's interests; the informational undermining of trust in international alliances and partnerships.

Thus, the purpose of the information policy of Ukraine is the activity of state authorities concerning the creation, collection, obtaining, storage, use, distribution, and protection of information data (Law of Ukraine No. 2657-XII, 1992). The hybrid information war is a threat to national security (Law of Ukraine No. 2469-VIII, 2018).

Therefore, a lot of attention should be paid to cyber security, that is, the implementation of policies, processes, and technologies to protect organizations, their critical systems and confidential information from digital attacks (Law of Ukraine No. 2163-VIII, 2017). The main task in improving this structure is to preserve the cyber stability and cyber security

of the set of state information institutions, management systems, and communication in the digital transformation (Decree of the President of Ukraine No. 392/2020, 2020).

The Ministry of Culture and Information Policy of Ukraine has broad powers in the coordination of information security in Ukraine. Part of the coordination functions is assigned to the National Security and Defence Council of Ukraine (the NSDC) (Law of Ukraine No. 183/98-BP, 1998).

In turn, the State Committee for Television and Radio Broadcasting of Ukraine is responsible for the creation and implementation of a national course in the field of television and radio broadcasting (Resolution of the Cabinet of Ministers of Ukraine No. 341, 2014).

The Ministry of Digital Transformation and the Committee on Digital Transformation of Ukraine carry out a huge amount of work on cyber security. Considering the discretion of the powers of state bodies, planning Ukraine's state information policy in the cyber security sphere in conditions of direct aggression by the Russian Federation should contain mandatory components (Figure 4).

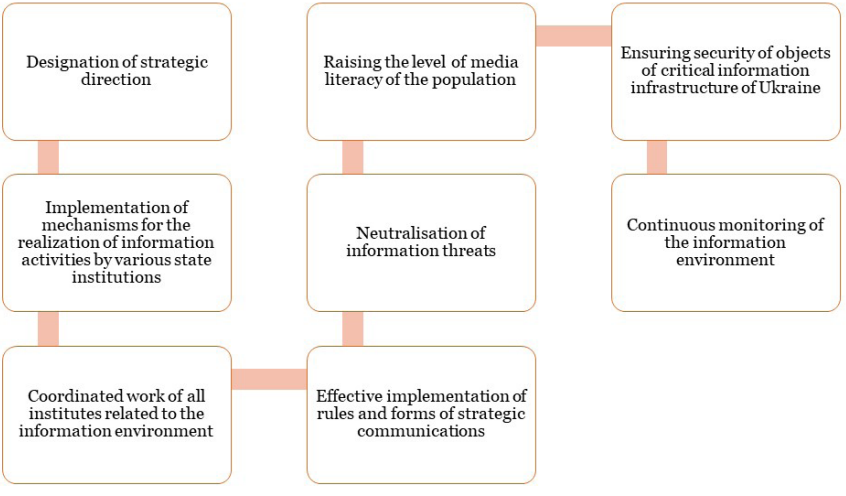

Figure 4: Mandatory components of planning the state information policy of Ukraine in the cyber security sphere in conditions of direct aggression by the Russian Federation (compiled by the authors).

Ukraine is making a lot of efforts to improve the planning of information policy in the cyber security sphere. In December 2021, the Information

Security Strategy of Ukraine was put into effect (Decree of the President of Ukraine No. 685/2021, 2021). Accordingly, on August 11, 2022, the Ministry of Culture and Information Policy of Ukraine proposed a public discussion of the draft Strategy implementation plan.

In March 2021, the Centre for Strategic Communication and Information Security was established under the Ministry of Culture and Information Policy of Ukraine. On March 11, 2021, the Centre for Countering Disinformation was established in Ukraine (Decree of the President of Ukraine No. 106/2021, 2021). Its main areas of activity include immediate notification of the population; detection of disinformation and manipulation; guarantee of information security; fight against information terrorism.

There are also some Ukrainian non-governmental organizations, engaged in fact-checking: "StopFake", "VoxUkraine", "FactCheck" and "Slovo i Dilo". On March 19, 2022, considering Russia's direct military aggression and the martial law, the President of Ukraine V. Zelensky signed a decree on the unification of all national TV channels into one platform according to the decision of the NSDC on the implementation of a single information policy (Decree of the President of Ukraine No. 152/2022, 2022).

Round-the-clock information is presented on the consolidated platform "United News". The decree also stops the activities of private media companies. The goal of the development of a unified information platform is to counteract the active spread of disinformation that justifies or refutes the armed aggression of the Russian Federation against Ukraine.

The modern development of cyberspace in Ukraine is influenced by both civilizational and specific components, which are a consequence of the hybrid threat from the Russian Federation. In Ukraine, a list of categories of cyber incidents has been developed (Computer Emergency Response Team of Ukraine, 2021).

These include malicious (offensive) content, malicious software code, collection of information by an intruder, attempts to interfere, interference, violation of accessibility, violation of properties of information, fraud, and known vulnerability. Since the beginning of the war, 796 cyber-attacks have been carried out in Ukraine (State Service of Special Communications and Information Protection of Ukraine, 2022). Government and local authorities were most often subjected to attacks – 179 times, the defence sector was attacked 104 times, the financial sector – 55 times, energy sector – 54 times. The most common methods of cyberattacks were the collection of information by an intruder – 242 times, malicious software code – 192 times, interference – 92, attempts to interfere – 82 times, and violation of accessibility – 56 times.

The Cyber Security Strategy of Ukraine was approved on August 26, 2021 (Decree of the President of Ukraine No. 447/2021, 2021). On February 1, 2022, the plan for implementing the Strategy was put into effect (Decree of the President of Ukraine No. 37/2022, 2022), which defines strategic goals: effective cyber defence; protection against cybercrime and cyberterrorism; implementation of appropriate deterrence mechanisms; high-quality technical knowledge in the cyber security sphere; protection of digital public services; increasing the level of appropriate coordination; development of international cooperation in this field.

A set of measures for the implementation of the plan should be carried out annually with corresponding indicators of implementation based on the best practices of the USA and EU member states and considering modern challenges in the cyber security sphere. A lot of attention was paid to the establishment of systematic exchange of information on destructive activities in cyberspace and the development of cooperation with the USA, EU member states and NATO member states. Information on the state of implementation of the plan must be provided to *the National Coordination Centre* for *Cybersecurity* (Decree of the President of Ukraine No. 96/2016, 2016).

To counter hybrid threats, the decision of the NSDC of May 14, 2021, provides for the creation of cyber troops within the structure of the Ministry of Defence of Ukraine (Decree of the President of Ukraine No. 446/2021, 2021). The establishment of the National Centre for Reserving State Information Resources in 2021 was an important step forward cyber security (Resolution of the Cabinet of Ministers of Ukraine No. 94, 2021). The strategic task on implementation of the state information policy and ensuring information security of Ukraine in the cyber protection sphere and its main problem is to increase the level of coordination of activities of all state institutions in the information space.

Unlike the European Union or other international organizations, the national governments of the member states have the necessary tools, including intelligence and counter-intelligence agencies (both civilian and military), security forces (enforcement of public order and security), means of communication with citizens and capacities to counter hybrid threats.

At the same time, while national security is a vital concern of each member state, hybrid threats often transcend borders, leaving the EU with a critical complementary role in supporting member states' efforts. In April 2016, the European Commission presented the Joint *Framework* on *Countering Hybrid Threats* (Joint Communication to the European Parliament and the Council, 2016). In June 2018, the European Commission published the *Joint Communication* on *increasing resilience* and bolstering *capabilities* to address *hybrid threats* (Joint Communication to the European Parliament, the European Council and the Council, 2018).

The EU's strategic agenda for 2019-2024 clearly emphasizes resilience to hybrid threats and disinformation as one of the key areas of future work.

In December 2019, the European Council Conclusions on complementary efforts to enhance resilience and counter hybrid threats were adopted (Council of the European Union, 2019), which states the possibility for member states to invoke the EU solidarity clauses when dealing with a serious crisis caused by hybrid threats. The Security Union Strategy adopted by the EU (EUR-Lex, 2020) is based on coordinated EU support to member states on several issues, ranging from organized crime and terrorism to cyber security and hybrid threats.

The European Parliament has also established a Special Committee on Foreign Interference in All Democratic Processes in the EU, including Disinformation (INGE). With a strong political mandate and a high-profile political platform, the INGE Committee can provide visibility and political support to the EU's efforts to investigate and counter foreign interference, including through a series of hearings, testimony sessions and public debates.

The European Union states that Russia's military aggression against Ukraine is accompanied by information manipulation and interference (European Commission, 2022a). There is a constant risk of manipulation of audio-visual materials and disinformation, which Russia may try to use as a pretext for new military attacks, resulting in the weakening of determination and unity of the Ukrainian people, division of the international community in its rejection of the war, and the emergence of doubts about Russia's violations of international law.

The Strategic Compass (ANNEX, 2022), commits the EU to react harshly to foreign information manipulation and interference, to increase its resilience and ability to counter such threats. Russia's aggressive war against Ukraine has strengthened cooperation in the field of cyberspace. In this regard, the European External Action Service (EEAS) and the *European Union Agency* for *Cybersecurity* (ENISA) are working on sharing, situational awareness and coordinating responses to malicious cyber activities against Ukraine.

They also work on supporting Ukraine and other countries in the region by working with partners, including the US and NATO, to ensure complementarity. The creation of the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) in April 2017 was a notable event in EU-NATO cooperation. This organization is a key contributor to the deepening of trust and information sharing between the EU and NATO at the strategic level, the expansion of the EU's research and analytical capacity, as well as the organization of joint exercises for strengthening training capabilities and resilience to counter a hybrid intervention.

The work on exposing Russia's manipulations was intensified, in particular, through the EUvsDisinfo website. From March 2, 2022, the broadcasting of the Russian state media RT and Sputnik channels in the EU or diverted to the EU was stopped. Online platforms, leading social networks, advertisers, and the advertising industry, which signed the Code of Practice on Disinformation (European Commission, 2022b), are taking urgent measures to limit disinformation related to Russian aggression against Ukraine.

The EU works closely with its Member States through the EU Rapid Alert System and the G7 Rapid Response Mechanism, as well as with international partners such as NATO, the US, Canada, to share information on Russia's manipulation tactics.

The European Digital Media Observatory (EDMO) created a disinformation task force after the outbreak of war in Ukraine and coordinates fact-checkers and researchers across its network. This format provides for the annual approval of the NATO-Ukraine National Cooperation Program at the state level. Effective civil society engagement may strengthen social resilience, including through efforts to support information pluralism, investing in civic awareness through education, and supporting an independent press that responds quickly to any disinformation.

A successful example of such cooperation in the Baltic States was the involvement of investigative media "Re:Baltica" (2020) in official fact-checking for Facebook, which helped to detect and prevent the rapid, uncontrolled spread of malicious content.

4. Discussion

It may be concluded that hybrid threats are multifaceted, ambiguous and hidden by nature, which makes them very difficult to contain, identify, counter or attribute (Bērziņa Čerenkova *et al*., 2019). The main task of the hybrid threat is not to directly confront the state or attack it, which would lead to an immediate response, but to weaken the country's determination to confront through covert means of intervention, aimed at undermining the internal cohesion of the state (Wigell, 2019). Hybrid threats are a constant feature of today's security environment and part of the current security landscape of the EU, NATO, and Eastern Partnership countries. Joint adaptation to future challenges will mark the transition to a better vision of security and strengthen strategic thinking regarding hybrid threats (Ratsyborinska, 2022).

The nature of hybrid threats is constantly changing, which requires continuous vigilance. Most countries need to develop a more strategic

approach to countering hybrid threats, implement national adjustments, and develop active community participation (Bajarūnas, 2020). The Euro-Atlantic governments and institutions should develop a more effective and comprehensive transatlantic counter-hybrid strategy in cooperation with the private sector and civil society to strengthen their counter-hybrid capacity.

These activities range from organizational initiatives at the national and international levels to functional efforts related to resourcing, training, adoption of laws and their implementation. Due to the strengthening of hybrid threats shortly, including in the aftermath of the coronavirus crisis, transatlantic policymakers should consider this agenda an urgent priority (Speranza, 2020).

Key international organizations should work together with various states both within and outside international organizations and ensure cooperation between sectors and levels (Nilsson *et al*., 2021). According to scientists, this requires cooperation between the military, political, economic, civil and information spheres both in the public and private sectors, as well as at the local, regional, national, and international levels.

The need to collect qualitative information and carry out its multi-level assessment and verification was established in the study. Scientists believe that policymakers must precisely set the rigidity of restrictions within which the intended policy will be implemented (Howlett, 2019). In the case of short-term policy goals, the task of developers is to accurately assess the rigidity of current restrictions and include this information into the design process at the right time (Maor, 2020).

When it comes to long-term policy goals, the challenge is to establish, which restrictions cannot be changed, which restrictions can be ignored, and which ones can be changed (and how) at the beginning of their realization to increase the chances of policy success. After that, this information, according to the scientist, should be fully incorporated into the design process at the appropriate time.

It can be concluded that carefully developed cyber protection should be used for the information security of objects for different purposes. This applies to both the protection of the object itself and the protection of the information circulating in it (Zvezdova and Vakalyuk, 2022). Future ups and downs in countering disinformation will be determined mainly by the development of public-private partnerships, especially through cooperation with the largest online platforms (Szymański, 2020).

Close collaboration with the private sector is the vital long-term impact of any legal framework that may be developed to address hybrid threats (Lonardo, 2021). According to the scientist, hybrid threats may lead to the era of privatization of security and defence, or, at least, to the spread of basic government functions in the private sector.

The implementation in Ukraine of a virtual educational laboratory for modelling processes in information policy for the needs of state and private cyber security will become an effective tool in social processes. This will allow Ukraine to move along its educational trajectory and will expand the range of educational tasks and enrich them with modern content (Arsenovych, 2021).

Conclusions

State information policy should reflect current problems that have emerged in the sphere of information security in the international arena. It is necessary to implement legal and regulatory protection of the rights and interests of all subjects of information relations, namely individuals, social groups, society, and the state in general. The planning of changes in information management should ultimately contribute to the achievement of common national goals and priorities.

Improvement of current planning of information policy in cyber security depends on the strategic approach, goals and context, and should be based on unified conceptual principles. When planning information policy, it is necessary to consider justifications and sets of arguments, which form the basis of the corresponding policy in the field of cyber security.

Russia's aggressive war against Ukraine has shown how quickly theoretical threats can become real and stressed the importance of vigilance, coordination, and readiness. In the conditions of a hybrid war, the state that has become the object of aggression should make every effort to neutralize the corresponding threats. The conflict with the Russian Federation showed that the state information policy of Ukraine is aimed at restoring the sovereignty and territorial integrity of Ukraine, ending the conflict, and stabilizing the post-conflict socio-political situation.

Special attention is paid to constant objective monitoring of the information environment, outlining the strategic narrative and coordination of work of all state institutions in the information space. The planning includes the principles and methodology of strategic communications, detection, assessment and forecasting of the consequences of information threats, security guarantees for the objects of critical information infrastructure of Ukraine and raising media literacy of the population.

The improvement of information policy planning in the field of cyber security is also based on the need to develop a system of relevant views and determination of the action plan of the military-political leadership of Ukraine.

The strategic task of implementation of the state information policy and ensuring Ukraine's information security in the field of cyber protection is also to increase the level of coordination of the activities of all state institutions in the information space. The cross-border nature of cyber threats contributes to the strengthening of international cooperation between countries. National and supranational initiatives in the field of information cyber security can be involved in the planning of the information policy of states and may become the object of further studies.

Bibliographic References

ANNEX. 2022. A Strategic Compass for Security and Defence - For a European Union that protects its citizens, values and interests and contributes to international peace and security (Vol. 7371/22). General Secretariat of the Council. Brussels, Belgium.

ARSENOVYCH, Levon. 2021. "Ways of forming a system of personnel training in the field of cyber security of the state authorities of Ukraine in the conditions of the development of the digital society of Ukraine" In: Actual problems of state information security management: a collection of theses of scientific reports. XII All-Ukrainian scientific and practical conference. National Academy of the Security Service of Ukraine. Kyiv, Ukraine.

BAJARŪNAS, Eitvydas. 2020. "Addressing Hybrid Threats: Priorities for the EU in 2020 and Beyond" In: European View. Vol. 19, No. 1, pp. 62-70.

BALCAEN, Pieter; DU BOIS, Cind; BUTS, Caroline. 2022. "A Game-theoretic Analysis of Hybrid Threats" In: Defence and Peace Economics. Vol. 33, No. 1, pp. 26-41.

BĒRZIŅA ČERENKOVA, Una Aleksandra; PAMMENT, James; SAZONOV, Vladimir; GRANELLI, Francesca; ADAY, Sean; ANDŽĀNS, Māris; GRAVELINES, John-Paul; HILLS, Mils; HOLMSTROM, Miranda; KLUS, Adam; MARTINEZ-SANCHEZ, Irene; MATTIISEN, Mariita; MOLDER, Holger; MORAKABATI, Yeganeh; SARI, Aurel; SIMONS, Gregory; TERRA, Jonathan. 2019. Hybrid Threats: A Strategic Communications Perspective. Riga: NATO Strategic Communications Centre of Excellence. Available online. In: https://stratcomcoe.org/publications/hybrid-threats-a-strategic-communications-perspective/79. Consultation date: 15/04/2022.

BONDAR, Hanna; RAKUTINA, Liudmyla. 2019. "Information policy and information security" In: Public Administration and Customs

Administration. Vol. 4, No.23, pp. 42-49. Available online. In: https://doi.org/10.32836/2310-9653-2019-4-42-49. Consultation date: 15/04/2022.

CISCO CYBERSECURITY REPORT. 2020. Securing What's Now and What's Next: 20 Cybersecurity Considerations for 2020. CISO Benchmark Study. Available online. In: https://www.cisco.com/c/dam/m/en_hk/ciscolive/2020-ciso-benchmark-cybersecurity-series.pdf. Consultation date: 15/04/2022.

COMPUTER EMERGENCY RESPONSE TEAM OF UKRAINE. 2021. List of categories of cyber incidents. Available online. In: https://cert.gov.ua/recommendation/16904. Consultation date: 15/04/2022.

COUNCIL OF THE EUROPEAN UNION. 2019. Council Conclusions on complementary efforts to Enhance Resilience and Counter Hybrid Threats (Vol. 14972/19). Brussels. Available online. In: https://data.consilium.europa.eu/doc/document/ST-14972-2019-INIT/en/pdf. Consultation date: 15/04/2022.

DECREE OF THE PRESIDENT OF UKRAINE dated March 15, 2016 No. 96/2016. On the decision of the National Security and Defense Council of Ukraine dated January 27, 2016 "On the Cybersecurity Strategy of Ukraine". Available online. In: https://www.president.gov.ua/documents/962016-19836. Consultation date: 15/04/2022.

DECREE OF THE PRESIDENT OF UKRAINE dated September 14, 2020 No. 392/2020. On the decision of the National Security and Defense Council of Ukraine dated September 14, 2020 "On the National Security Strategy of Ukraine". Available online. In: https://zakon.rada.gov.ua/laws/show/392/2020#n7. Consultation date: 15/04/2022.

DECREE OF THE PRESIDENT OF UKRAINE. 2021. No. 106/2021. On the decision of the National Security and Defense Council of Ukraine dated March 11, 2021 "On the establishment of the Center for countering disinformation". Available online. In: https://www.president.gov.ua/documents/1062021-37421. Consultation date: 15/04/2022.

DECREE OF THE PRESIDENT OF UKRAINE. 2021. No. 446/2021. On the decision of the National Security and Defense Council of Ukraine dated May 14, 2021 "On urgent measures for the cyber defence of the state". Available online. In: https://zakon.rada.gov.ua/laws/show/446/2021#n5. Consultation date: 15/04/2022.

DECREE OF THE PRESIDENT OF UKRAINE. 2021. No. 447/2021. On the decision of the National Security and Defense Council of Ukraine dated

May 14, 2021 "On the Cybersecurity Strategy of Ukraine". Available online. In: https://zakon.rada.gov.ua/laws/show/447/2021#n7. Consultation date: 15/04/2022.

DECREE OF THE PRESIDENT OF UKRAINE. 2021. No. 685/2021. On the decision of the National Security and Defense Council of Ukraine dated October 15, 2021 "On Information Security Strategy". Available online. In: https://www.president.gov.ua/documents/6852021-41069. Consultation date: 15/04/2022.

DECREE OF THE PRESIDENT OF UKRAINE. 2022. No. 152/2022. On the decision of the National Security and Defense Council of Ukraine dated March 18, 2022 "Regarding the implementation of a unified information policy under martial law". Available online. In: https://zakon.rada.gov.ua/laws/show/152/2022#n2. Consultation date: 15/04/2022.

DECREE OF THE PRESIDENT OF UKRAINE. 2022. No. 37/2022. On the decision of the National Security and Defense Council of Ukraine dated December 30, 2021 "On the Implementation Plan of the Cybersecurity Strategy of Ukraine". Available online. In: https://zakon.rada.gov.ua/laws/show/37/2022#Text. Consultation date: 15/04/2022.

DRAGOS, Valentina; FORRESTER, Bruce; REIN, Kellyn. 2020. "Is hybrid AI suited for hybrid threats? Insights from social media analysis" In: 2020 IEEE 23rd International Conference on Information Fusion (pp. 1-7). Available online. In: https://dx.doi.org/10.23919/FUSION45008.2020.9190465. Consultation date: 15/04/2022.

EUR-LEX. 2020. Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy. COM/2020/605 final. Brussels. Available online. In: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0605. Consultation date: 15/04/2022.

EUROPEAN COMMISSION. 2022a. Communication from the Commission to the European Parliament and the Council on the Fourth Progress Report on the implementation of the EU Security Union Strategy. COM (2022) 252 final. Brussels. Available online. In: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022DC0252. Consultation date: 15/04/2022.

EUROPEAN COMMISSION. 2022b. The 2022 Code of Practice on Disinformation. Available online. In: https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation. Consultation date: 15/04/2022.

HLUSHKO, Alina; PANTAS, Vasyl; BABENKO, Sofiia. 2022. "Information policy in the system of ensuring financial security of the state" In: Efektyvna ekonomika. Vol. 2. Available online. In: https://doi.org/10.32702/2307-2105-2022.2.95. Consultation date: 15/04/2022.

HOWLETT, Michael. 2019. Designing Public Policies: Principles and Instruments (2nd Ed.). Routledge. London, UK.

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL. 2016. Joint Framework on countering hybrid threats a European Union response. JOIN/2016/018 final. Brussels. Available online. In: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018. Consultation date: 15/04/2022.

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL. 2018. Increasing resilience and bolstering capabilities to address hybrid threats. JOIN/2018/16 final. Brussels. Available online. In: https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:52018JC0016. Consultation date: 15/04/2022.

KALNIETE, Sandra; PILDEGOVIČS, Tomass. 2021. "Strengthening the EU's resilience to hybrid threats" In: European View. Vol. 20, No. 1, pp. 23–33.

LAW OF UKRAINE. 1992 No. 2657-XII. On Information. Available online. In: https://zakon.rada.gov.ua/laws/show/2657-12#Text. Consultation date: 15/04/2022.

LAW OF UKRAINE. 1998. No. 183/98-BP. On the National Security and Defense Council of Ukraine. Available online. In: https://zakon.rada.gov.ua/laws/show/183/98-%D0%B2%D1%80#Text. Consultation date: 15/04/2022.

LAW OF UKRAINE. 2017. No. 2163-VIII. On the basic principles of ensuring cyber security of Ukraine. Available online. In: https://zakon.rada.gov.ua/laws/show/2163-19#Text. Consultation date: 15/04/2022.

LAW OF UKRAINE. 2018. No. 2469-VIII. On National Security of Ukraine. Available online. In: https://zakon.rada.gov.ua/laws/show/2469-19#Text. Consultation date: 15/04/2022.

LONARDO, Luigi. 2021. "EU Law Against Hybrid Threats: A First Assessment" In: European Papers. Vol. 6, No. 2, pp. 1075-1096.

LUO, Han; CAI, Meng; CUI, Ying. 2021. "Spread of Misinformation in Social Networks: Analysis Based on Weibo Tweets" In: Security and Communication Networks. https://doi.org/10.1155/2021/7999760 Available online. In: https://www.hindawi.com/journals/scn/2021/7999760/. Consultation date: 15/04/2022.

MAOR, Moshe. 2020. "Policy over- and under-design: an information quality perspective" In: Policy Sciences. Vol. 53, pp. 395-411.

NILSSON, Niklas; WEISSMANN, Mikael; PALMERTZ, Björn; THUNHOLM, Per; HÄGGSTRÖM, Henrik. 2021. "Security challenges in the grey zone: Hybrid threats and hybrid warfare" In: WEISSMANN, Mikael; NILSSON, Niklas; PALMERTZ, Björn; THUNHOLM, Per (Eds.), Hybrid Warfare: Security and Asymmetric Conflict in International Relations (pp. 1-18). London, UK.

RATSYBORINSKA, Vira. 2022. "EU-NATO and the Eastern Partnership countries against hybrid threats (2016-2021)" In: National Security and the Future. Vol. 23, No. 2, pp. 144-156.

RE:BALTICA. 2020. Re:Check kļūst par oficiālajiem FB faktu pārbaudes partneriem. Available online. In: https://rebaltica.lv/2020/03/recheck-klust-par-oficialajiem-fb-faktu-parbaudes-partneriem/. Consultation date: 15/04/2022.

RESOLUTION OF THE CABINET OF MINISTERS OF UKRAINE. 2014. No. 341. On approval of the Regulations on the State Committee for Television and Radio Broadcasting of Ukraine. Available online. In: https://zakon.rada.gov.ua/laws/show/341-2014-%D0%BF#Text. Consultation date: 15/04/2022.

RESOLUTION OF THE CABINET OF MINISTERS OF UKRAINE. 2021. No. 94. On the implementation of an experimental project on the functioning of the National Center for Reservation of State Information Resources. Available online. In: https://zakon.rada.gov.ua/laws/show/94-2021-%D0%BF#n8. Consultation date: 15/04/2022.

SPERANZA, Lauren. 2020. A Strategic Concept for Countering Russian and Chinese Hybrid Threats. Washington, D.C.: Atlantic Council, Scowcroft Center for Strategy and Security, July. Available online. In: https://www.atlanticcouncil.org/wp-content/uploads/2020/07/Strategic-Concept-for-Countering-Russian-and-Chinese-Hybrid-Threats-Web.pdf. Consultation date: 15/04/2022.

STATE SERVICE OF SPECIAL COMMUNICATIONS AND INFORMATION PROTECTION OF UKRAINE. 2022. Four months of war: statistics of cyberattacks. Available online. In: https://cip.gov.ua/ua/news/chotiri-misyaci-viini-statistika-kiberatak. Consultation date: 15/04/2022.

SZYMAŃSKI, Piotr. 2020. Towards greater resilience: NATO and the EU on hybrid threats. OSW Commentary 2020-04-24. UNSPECIFIED. Available online. In: http://aei.pitt.edu/id/eprint/103308. Consultation date: 15/04/2022.

TAHERDOOST, Hamed; MADANCHIAN, Mitra; EBRAHIMI, Mona. 2021. "Advancement of Cybersecurity and Information Security Awareness to Facilitate Digital Transformation: Opportunities and Challenges" In: SANDHU, Kamaljeet (Ed.), Handbook of Research on Advancing Cybersecurity for Digital Transformation (pp. 99-117). IGI Global. Available online. In: https://doi.org/10.4018/978-1-7998-6975-7.ch006. Consultation date: 15/04/2022.

VARONIS. 2022. 166 Cybersecurity Statistics and Trends (updated 2022). Available online. In: https://www.varonis.com/blog/cybersecurity-statistics. Consultation date: 15/04/2022.

VESELOVA, Liliia. 2021. "Administrative and legal foundations of cyber security in conditions of hybrid warfare" In: Dissertation for the Doctor of Law degree. Odesa: Odessa State University of Internal Affairs. Available online. In: http://oduvs.edu.ua/wp-content/uploads/2016/06/Disertatsiya_Veselovoi_L.YU..pdf. Consultation date: 15/04/2022.

WIGELL, Mikael. 2019. "Hybrid interference as a wedge strategy: a theory of external interference in liberal democracy" In: International Affairs. Vol. 95, No. 2, pp. 255–275.

WIJNJA, Kim. 2022. "Countering hybrid threats: does strategic culture matter?" In: Defence Studies. Vol. 22, No. 1, pp. 16-34.

ZVEZDOVA, Olesia; VAKALYUK, Olexander. 2022. "A strategy for ensuring cyber security in hybrid warfare" In: Acta De Historia & Politica: Saeculum. Vol. XXI, No. 03, pp. 82-90.

UNIVERSIDAD DEL ZULIA

CUESTIONES POLÍTICAS

Vol.40 Nº 74

Esta revista fue editada en formato digital y publicada en octubre de 2022, por el ***Fondo Editorial Serbiluz, Universidad del Zulia. Maracaibo-Venezuela***

www.luz.edu.ve
www.serbi.luz.edu.ve
www.produccioncientificaluz.org