COMMUNICATION & SOCIETY

Petro Katerynych
https://orcid.org/0000-0002-5967-2368
katerinich1993@gmail.com
Mariupol State University

Submitted
February 8th, 2022
Approved
June 3rd, 2022

© 2022
Communication & Society
ISSN 0214-0039
E ISSN 2386-7876
doi: 10.15581/003.35.4.37-53
www.communication-society.com

2022 – Vol. 35(4)
pp. 37-53

How to cite this article:
Katerynych, P. (2022). Comparative analysis of the information security environment in Ukraine and Poland (survey of journalists and editors). *Communication & Society, 35*(4), 37-53.

Comparative analysis of the information security environment in Ukraine and Poland (survey of journalists and editors)

Abstract

Information security of Ukraine and Poland with the beginning of the Russian Federation's armed aggression against Ukraine is sensitive to various forms of information threats. Information attacks by the aggressor country accompany the challenges of the full-scale war that exploded within Eastern Europe. Active military actions on the territory of Ukraine, the migrant crisis on the border with Poland –all this tests both countries' information environment for resilience. Journalists play an essential role in the process of information defense. In the study, we compare legal acts and governmental regulations of Ukraine and Poland in the field of information security in order to identify the current state of information security environment in both countries. In our work, we analyze the concept of "information security" in scientific studies of Ukrainian and Polish researchers, as well as in normative legal acts. Journalists and editors of leading Ukrainian and Polish media outlets were questioned about their attitudes toward existing information security doctrines and strategies. It was found that journalists of both countries (n = 46, α(ua)=0.75; α(pl)=0.78) find the tools of protection against information threats insufficient, consider the participation of journalists in the formation of information policy significant, and also consider as risky the possibility to adopt documents that would describe the social responsibility of journalists in conditions of information aggression.

Keywords
Information warfare, information environment, Ukraine, Poland, information security, journalists' survey.

1. Introduction

Ukraine's information security system, which was only actively developed in late 2014, is sensitive to various information threats because it had not previously been tested in harsh war conditions. The crisis that the information security system is experiencing is primarily due to the inability to find the right tactics to counter threats and counterattacks. Some researchers even believe that Ukraine lacks an information security system that could provide identification, analysis of information threats to national security, as well as effective counteraction to these threats (Golovchenko *et al.*, 2018; Shemchuk, 2019; Zolotar *et al.*, 2021).

The Information Security Doctrine was first enacted in Ukraine in 2016, and a new version has been under development since 2020. Given the escalation of hybrid warfare into a full-scale war, in Ukraine the new version of the Information Security Doctrine has identified the following urgent threats to the national security of Ukraine in the information sphere: implementation of special information operations aimed at undermining the defense capability, demoralization of the personnel of the Armed Forces of Ukraine and other military; fuelling panic moods, aggravation and destabilization of the sociopolitical and socio-economic situation, inciting interethnic and inter-confessional conflicts in Ukraine; conducting special information operations in other countries by the aggressor-state to create a negative image of Ukraine in the world; information invasion by the aggressor state and the structures it controls, in particular by expanding its own information infrastructure on the territory of Ukraine and in other states; The aggressor state's information predominance in the temporarily occupied regions; insufficient development of national information infrastructure, which limits Ukraine's ability to effectively counter information aggression; ineffectiveness of the state information policy, shortcomings in legislation on the regulation of social relations in the information sphere, uncertainty of the strategic narrative, insufficient level of media culture of society; spread of calls for radical actions, propaganda of isolationist and autonomist concepts of coexistence of Ukrainian regions, spreading of radical actions, pro-federalism and separatism in Ukraine. (Decree of the President of Ukraine..., 2017).

In 2013, Poland's Internal Security Agency published a strategic document –the "White Book of National Security," which describes models of interaction between state institutions and the security environment (economic, energy, environmental, information). In the same year, Poland's National Security Bureau proposed for discussion a draft of the Information Security Doctrine, concluded in connection with the "escalation of hybrid threats, including information threats –propaganda, disinformation, psychological intimidation by other countries and non-state actors (e.g., terrorist organizations)" (Draft Doctrine..., 2015). However, the Doctrine was never enacted. The threats to Poland's information space are outlined in the section of the Polish National Security Strategy (2020).

We define the country's information security as a multi-vector security sector, the purpose of which is the country's security in the information space through control in its own, internal, state information sphere and adequate protection of state interests in the external (international) infosphere (Internal and External Situation..., 2014). As we investigate conceptual and applied aspects of information security of Ukraine and Poland and find out the attitude of media representatives to the structure of information security of Ukraine and Poland, we faced four research questions:

RQ1. What is the information security environment of Ukraine and Poland?

RQ2. Are Ukrainian journalists familiar with the Information Security Doctrine of Ukraine, how effective do they consider it and are they ready to join the process of updating the Doctrine?

RQ3. Are Polish journalists familiar with the provisions on information security contained in the Polish National Security Strategy/Draft of the Information Security Doctrine, how effective do they consider it and are they ready to join the process of updating?

RQ4. Do Ukrainian and Polish journalists consider the state regulation of journalists' social responsibility in conditions of information war?

2. Methodology

The survey of Ukrainian and Polish journalists and editors, conducted in 2021 and early 2022, helped us to obtain important data for the analysis of the problem under study, allowed us to determine whether Ukrainian journalists are familiar with such an important document as the Information Security Doctrine of Ukraine, and Polish journalists –with the provisions regarding information security contained in the Polish National Security Strategy and the draft of the Information Security Doctrine of Poland. We also asked journalists in both countries whether it is significant to develop documents that define the social responsibility of journalism in the face of information threats. It was also valuable to survey national media workers about the possible application of information security documents in their daily activities and the potential influence of media owners on journalists' and editors' compliance with the principles and standards of information security described in the government documents discussed in this article.

The preparatory stage of the survey included the development of questions, drawing up questionnaires. The next stage was the distribution of questionnaires. The links to answer the questionnaire in electronic form were sent to selected journalists by personal message on Facebook Messenger, Telegram, WhatsApp, and personal e-mails of journalists and editors. The request to complete the survey included information about the purpose of the study, a description of how the results would be used and brief information about what personal data and how exactly would be used. We did not send messages with a request to take part in the survey to editorial and corporate e-mail addresses or contact forms on websites, as we believed that this could result in pressure from the editorial office or media owners on journalists and editors who wished to answer questions. The journalists answered the questionnaire online (access was only possible if you received a link). It was possible to answer only once from one IP address. We know the names of the journalists who took the questionnaire, but to protect their data, we only indicate the name of the media outlet and their work experience (employment time as a journalist, editor, analyst...) in the results processing form. At the beginning of the questionnaire, we specified the purpose of data collection, the format in which processing would take place, and what personal data would be used in the study. All respondents agreed that they answered the questions independently, and they did not experience any pressure from the editorial office or a third party when completing the answers.

A total of 60 survey invitations were sent to journalists and editors in both countries (n=120). In order to take into account the diversity and balance of opinions, invitations were sent to employees of various national media outlets working in electronic media, print, television and radio. When sending the invitations, we used information available on open resources about the national media employees in Ukraine and Poland. The author of the research is fluent in Ukrainian and Polish, which allowed us to ensure effective communication with respondents, the preparation of questionnaires in two languages – Ukrainian and Polish–, and the appropriate processing of the results.

Our survey sample consists of journalists and editors of popular Ukrainian and Polish media who answered the questionnaire during late 2021 and early 2022. For Ukraine, the sample was 24 people (40% of those invited) representing 19 Ukrainian national media; for Poland, 22 people (36.6% of those invited) representing 16 Polish national media. Defining "journalist" can be a difficult task, as the boundaries of journalism are becoming increasingly blurred in the digital age (Molyneux & Zamith, 2020). The list included only those involved in the creation and production of content, namely correspondents, reporters, editors, content analysts, and presenters.

American researchers L. Molyneux and R. Zamith note the difficulties of interviewing journalists because of the specifics of the profession; in some cases the number of responses does not exceed single numbers (Molyneux & Zamith, 2020). A survey is an important tool for explaining correlations and allows for systematic comparisons between certain groups, as in our case. It is particularly well suited for questions that rely on scaling to draw statistical inferences and understand generalizations and relationships among variables. Journalist surveys most often examine journalists' perceptions of themselves, their work, and their environment (Molyneux & Zamith, 2020).

We used a self-created contact list to generate the sample. Because of resource and time constraints, researchers sometimes strive to narrowly define the target population to make a sampling frame. Researchers then apply an eligibility approach, systematically selecting the most relevant participants possible. This selection may include personal contact, sending a message, visiting each organization in the target population (Menke *et al.*, 2018), or searching for relevant contacts online (Dahmen *et al.*, 2018). Because it is usually easier to identify organizations than individuals, researchers frequently sample organizations first and then search for contacts in those organizations (Liu & Lo, 2018).

As L. Moluenuch and R. Zamith point out, it is important to send reminders to journalists about participating in the survey, this is crucial to ensure a high response rate; sending several reminder letters throughout the month will achieve the goal. According to L.Moluenuch and R. Zamith (2020),

> As such, it is unwise to wait under the assumption that journalists have added the survey to their to-do list. Often, they will be a willing participant if reminded at a different time, when they are either less busy or have a less-crowded inbox. Each reminder should include clear links to participate and to opt out of future mailings.

From the first time after sending invitations to take the survey, we received 12 responses (8 from Ukraine and 4 from Poland). The total number of completed questionnaires (n=46) was reached after the third round of sending invitations. Some researchers emphasize that surveys with lower response rates (about 20%) can produce more accurate results than surveys with higher response rates –about 60 or 70% (Visser *et al.*, 1996). The survey results we have conducted may not represent the opinion of all journalists in Ukraine or Poland. However, the participation in the survey of different rated media representatives with varying work experience allows us to draw some important conclusions from the data we have obtained.

The questionnaire begins with a "passport" –questions concerning the place of work (the name of the media), the time of work in the selected media (less than two years, two to five years, more than five years). The following questions record the answers to the scales we provided in the research questions. In the questionnaire, we used a unipolar Likert positional scale to form questions (for Ukrainian journalists: 9, for Polish journalists: 10). The difference in the number of questions is explained by the need to know the opinion of Polish respondents regarding 2 separate documents in the information security sector, the central part of questions (9 each) are the same for both groups of respondents. We also gave journalists the opportunity to answer one open-ended question, intended to find out the expanded opinion of respondents; 6 Polish respondents and 8 Ukrainian respondents gave an expanded answer (14 in total).

According to the number of participants, we used a group questionnaire. By the type of contact with the respondent, the questionnaire is remote. The correspondent method of questioning envisaged recording the responses received independently using an online form, further analysis of the results by the researcher using automatically generated statistics, and entering the final data into the table .xlsx.

To calculate the internal consistency of the survey questions, as well as to establish a wide range of reliability indicators, we calculate for all survey questions (all of which are constructed as scales from 1 (where 1 is a negative indicator, meaning – not familiar, not support) to 5 – positive indicator – knowledgeable, supportive), Cronbach's Alpha (or tau-equivalent reliability) factor. The coefficient is calculated using the tools of the SPSS program. The reliability score tells the researcher whether a respondent would give the same score on the same variable if that variable were to be rated again by the same respondent (Lavrakas, 2008). The calculation of Cronbach's Alpha (α) is the most common measure of internal consistency (likelihood) (Taber, 2018, p. 1273). Cronbach's Alpha is often determined when a researcher uses multiple Likert scale questions in a survey, and there is a need to know if such scales are reliable. Calculating the value of Cronbach's Alpha is common among social communication studies (Hanitzsch *et al.*, 2010).

3. Information security environment of Ukraine and Poland

Poland's information security environment during the Strategic National Security Review is defined as "well-defined and dynamic" already at the stage of analysis conducted in connection with the Review (the Strategic National Security Review is an analytical process that aims to develop substantial grounds for policy decisions) and, as a consequence, specific national security actions) (Strategic National, 2012). However, it should be noted that the White Book of National Security (*Biała Książka Bezpieczeństwa Narodowego*), published in 2013 as an outcome of the Strategic Review, does not define "hybrid war" (Bieliszczuk *et al.*, 2014). Therefore, as Professor Liedel (2015) notes, it was important to form appropriate definitions and offer them for public discussion "as concepts that define the international reality that surrounds us." Although these concepts have no legal weight at the international level nor at the state level, they can be the beginning of shaping responses to such threats.

According to "Hybrid Threats. How Poland's Environment is Changing" (Liedel, 2015),

> In Poland's case, this is important because the Russian-Ukrainian conflict, which is taking place beyond our eastern border, is a source of potential threats to the region's stability. This should not be forgotten even in the shadow of current events, such as the migration crisis that has been dragging on for a year, against which Europe is still unable to find a good cure. The geopolitical change arising from the evolution of Russian international policy remains a significant factor affecting the security of Poland and its citizens.

The White Paper of National Security is a strategic document that defines Poland's primary political and economic guidelines, understanding Poland's relations with the countries of interest. The document begins with an introduction by the President (then Bronisław Komorowski), followed by analytics (sections on internal and external threats, future cooperation with NATO and EU countries, other states, assessment of defense capabilities, and current geopolitical map). The paper states that Europe's security is determined by four factors: NATO, the EU, the U.S. strategic presence, and relations with Russia. NATO is likely to remain a powerful and effective political-military alliance planetary. The U.S. strategic (politico-military and economic) presence in Europe is the foundation of European security. Unknown coordinates arise from the increasingly visible U.S. strategic reorientation toward Asia and the Pacific (National Security Bureau, 2013).

A crucial external criterion influencing the state of Poland's security is the relationship between Russia and the West. Today, it is difficult to determine their clear perspective. Will Russia keep the course on developing a superpower, not considering others, mainly at the cost of its neighbors? Will there be a change of course in favor of cooperation to develop common security? Today, the most probable scenario is the continuation of the Russian policy, which is not advantageous for Poland (National Security Bureau, 2013).

It is not practiced in Ukraine to publish a comprehensive book of National Security. However, analytical base on this issue is monographs of the Institute for Strategic Studies, among others *World Hybrid War: Ukrainian Front*, *Ukraine and Russia: the Ninth Wall or the Chinese Wall*, *National Security of Ukraine: Evolution of Problems of Internal Policies*, analytical report *Ukraine's Foreign Policy in Crisis of the International Security Environment*. According to leading researchers of the Institute for Strategic Studies, Poland is a crucial partner of Ukraine in the geopolitical arena. Among such researchers are Dmytro Dubrov, Oleksandr Vlasiuk, Serhii Kononenko, Volodymyr Gorbulin, Borys Parakhonskyi, Halyna Yavorska (Horbulin *et al.*, 2015; Misko, 2017; Parakhonskyi & Yavorska, 2015; Vlasiuk, 2016).

European countries have lost and gained territory (Germany and Poland are prime examples), but this has not prevented them from being economically prosperous and politically stable. Territorial loss does not necessarily mean losing statehood (Horbulin *et al.*, 2015, p. 65). Poland has relatively the highest job losses due to Russian counter-sanctions, and the Baltic States have the highest losses in proportion to the size of their GDP (Misko, 2017, p.

425). Russia's aggression against Ukraine exposed NATO's vulnerability on its eastern flank (Poland, the Baltic States, and Northern Europe). The annexation of Crimea and further increased Russian military activity in the Black Sea created additional security threats for NATO member and partner countries in this region as well, forming a bridgehead for the spread of Russian influence towards the Mediterranean and the Middle East (Misko, 2017, p. 448).

Evgen Magda notes that Ukraine needs to produce interesting world meanings in the international information space while preserving its own identity. It is vital to preserve the foundations of national culture, while giving them a modern form. Magda (2015, pp. 29-30) writes,

> Today we observe a dialectical situation. On the one hand, interest in Ukraine has increased; the country no longer looks like a "gray area" in the center of Europe. On the other hand, the Ukrainian leadership is not carrying out effective reforms, disregarding narrow partisan or clan interests.

Poland's National Security Strategy identifies the Russian Federation as the aggressor, and Ukraine, Georgia, and Moldova as countries that Poland supports to in strengthening independence and pro-European aspirations (National Security Strategy, 2020, p.21). The Russian Federation is also named an aggressor in the National Security Strategy of Ukraine (2020), a strategic partnership is envisaged with the Republic of Azerbaijan, Georgia, the Republic of Lithuania, the Republic of Poland and the Republic of Turkey.

A broad definition of information security can be found in the book *Zarys teorii bezpieczeństwa narodowego* (Eugeniusz & Maciej, 2011, p. 103). The definition describes information security of Poland as a state of external and internal conditions that allow the free development of information society, and the conditions for achieving information security the authors call:

- security of the state's strategic resources;
- decisions of the authorities made based on reliable, up-to-date information;
- the unimpeded exchange of information between public authorities;
- uninterrupted operation of the network, information and communication technologies that create the critical teleinformation infrastructure of the state;
- state-guaranteed protection of classified information and personal data of citizens;
- the citizens' right to privacy, which public institutions do not violate;
- free access of citizens to public information.

Poland's National Security Strategy defines the key factors of information security:

- confidentiality (information is accessible only to authorized persons):
- integrity (means ensuring the accuracy, timeliness, and completeness of information and methods of its processing);
- accessibility (authorized persons have access to information and processing functions whenever legally required).

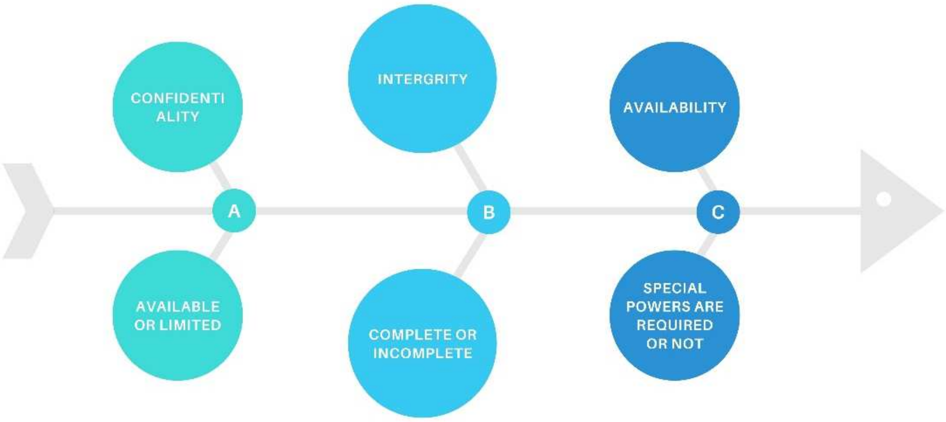
Assessing risks and threats, Poland's Internal Security Agency drafted an Information Security Doctrine in 2015. It is broader than the Ukrainian Doctrine and covers more relevant aspects. Even from the content, we can see that the Polish Doctrine provides for the consideration of the issue of information security in two sectors –internal and external–, which is, in our opinion, the right step because it allows to assess the degree and scope of information threats at the local and international levels. The researcher of the concept of "legal Doctrine" Semenihin (2018) states,

> Legal Doctrine is created as a result of fundamental scientific research related to deep and comprehensive analysis of the essence of state-legal phenomena and processes, clarifying the patterns of their emergence and development. This is the main reason for its high authority, a prerequisite for the legitimization of doctrinal provisions in the legal consciousness of lawyers, and, as a consequence, the perception of legal practice.

At the same time, legal Doctrine determines the system of views, ideas, and moral norms. Consequently, the document should contribute to the upgrade of the information reality; it is "security" that should become the presupposition in the phrase "information security."

Referring to the above sources, we can identify the following formula (Figure 1) of information security in Poland.

Figure 1. The formula of information security in Poland.



Source: The Polish National Security Strategy and the draft Doctrine of the Information Security Doctrine.

It is worth noting that the Polish formula corresponds to European standards in information security. The Dutch, Danish and German doctrines contain similar formulas. However, Germany has more categories of information privacy. The German government has added information warfare as one of the 4 threats of our time, this puts information policy on a par with international terrorism or illegal weapons proliferation. *Bundesamt für Sicherheit in der Informationstechnik* (BSI) – The Federal Office for Information Security distinguishes levels of information with special, limited, secret and open access.

In general, creating the main documents and regulations related to information security in both countries falls in 2015-2016. This is due to Russia's active information attacks against both countries (Sielezin, 2020).

In Ukraine, all laws related to information are subject to improvement, primarily the Law *On Information* (the most recent significant amendments to which were made in 2011), *On Access to Public Information* (the last significant amendments to which were made in 2011), *On Access to Public Information*, *On Protection of Information in Automated Systems*, *On News Agencies*, *On Print Media*, *On Scientific and Technical Information*... Including amendments to the Constitution. The upgrading of information legislation is one of the key moments in the information struggle at the legal level. These should not be casual actions of the Ministry responsible for information policy in Ukraine (such as creating of information troops having no legal status and formed voluntarily with low criteria for professional selection). The very notion of information security and its derivatives is subject to restructuring and restoration. This is confirmed by the Ukrainian Institute for Strategic Studies research: "the prerequisite for hybrid warfare is the formation of the broadest global socio-information and cultural space as a powerful mechanism for modeling reality..." (Misko, 2017).

The challenges of reality must be adequately responded to, so the concept of information security should be updated to meet the present challenges. Ihor Zaremba, Director of the Department of Industry, Industrial Infrastructure and State Property, notes that "today in Ukraine, unfortunately, the functions of public policy management in the information sphere are dispersed among at least 10 state institutions" (Transcript of the meeting…, 2017).

In the draft of the Polish Doctrine, we find assessments of the main information challenges risks and chances. The Ukrainian Doctrine has no such sections. The Polish Doctrine was developed by the Internal Security Agency (an analogue of the Security Service of Ukraine), the Ukrainian one by the Ministry of Information Policy (now the Ministry of Culture and Information Policy), and the National Security and Defense Council. In Poland until 2020, there was the Ministry of Digitization, which was responsible for the cybersecurity project for 2017-2022 and developed the Cybersecurity Strategy of the Republic of Poland for 2019-2024, its main goal is to increase the protection against cyber threats in the military and private sectors (The Cybersecurity Strategy…, 2019). In Ukraine, the Cyber Police was created in 2015, and in 2016 the Cybersecurity Strategy was put into effect by a decision of the National Security and Defense Council. This is especially relevant in light of the 2022 cyberattacks on Ukrainian government websites.

The purpose of the Information Security Doctrine of Ukraine is "information sovereignty" and "comprehensive information support for Ukrainian society." Information sovereignty in the Ukrainian Doctrine is defined as follows (Decree of the President of Ukraine…, 2017):

> The exclusive right of Ukraine in accordance with the Constitution and legislation of Ukraine and international law to determine and implement its domestic and geopolitical national interests in the information sphere, state domestic and foreign information policy, to form the infrastructure of national information space with its own information resources, to create conditions for integration into the world information space in compliance with the balance of interests of individuals, society and the state independently and freely.

For example, anti-Ukrainian campaigns in Crimea and Donbas began long before the occupation of these territories and the escalation (Razumkov Center, 2019). The concept or Doctrine should have provided a way out of the information stupor in which the citizens of Ukraine in these territories found themselves. High level of information noise, psychological information attacks from Russia, tense socio-economic situation, deformed public consciousness in the East of Ukraine, lack of real power, and regular army escalated the conflict. The information component plays an important role here –as there was no active response from Ukraine (work with the audience, formation of the so-called cultural meanings– which, according to Ukrainian expert Georgii Pocheptsov (2016), is an important stage in the war of meanings on the level of images and signs that aim to create distorted meanings of the enemy, the lack of national media ideology also affects the media image of the country (pp. 16-17).

The deformation of the public consciousness of the Donbas, its Russianization took place gradually, step by step, the effectiveness was achieved by playing on ethnic factors and the propaganda thesis of "the debauchery and demoralization of Europe," creating an information barrier to the perception of oneself as part of Europe. Ukrainian politics played into the hands of Russia. A powerful informational landmine was abolishing the law "*On the foundations of the state language policy*." It was out of time and gave Russia a key tool for creating propaganda and manipulating the ethnic consciousness of Ukrainians in the eastern regions.

According to Dmytro Dubov (2017), in all legislative initiatives from the field of information security of Ukraine, "information sovereignty" was considered one-sidedly, only within the national information policy, but it should have a broad regulation of action.

Dr. Katrin Nyman – Metcalf[1] concludes that the definition of information security in the Ukrainian Doctrine is quite broad and this is good because "some aspects of this concept are difficult to define narrowly" (Legal Analysis..., 2015).

The draft of the Polish Doctrine does not define information security in general, as it is done in Ukraine, but clarifies the content of the concept and narrows it down to "information security of the country." The definition in our translation is as follows (Draft Doctrine..., 2015):

> Information security of the country is a multi-vector security sector, the main content of which belongs to the information environment (including cyberspace); the process, the purpose of which is the security of the country in the information space through control in its own, internal, state information sphere and effective protection of state interests in the external infosphere. To achieve the goal, the following tasks should be realized: to ensure adequate protection of the available means of information and to safeguard against hostile disinformation propaganda actions (in the defense sector), while maintaining the ability to produce against possible adversaries (states or other entities) offensive actions in this area. These tasks are concretized in the information security strategy (doctrine) (operational and preparatory), and for their implementation, an appropriate information security system is maintained and developed.

As for the threats to information security in the Polish interpretation, these are also described in two dimensions –internal and external. Among the main external ones are "deformation of content and filling information systems with malicious logical content involving government communication channels or military control systems" (Draft Doctrine..., 2015). There is a close connection between information security and cybersecurity. Attacks on government communication channels are one of the mechanisms of information attacks. Let us recall the calls of Russian pranksters to Petro Poroshenko or Andrzej Duda. Among the external threats in the Polish doctrine draft are propaganda and disinformation, mainly spread through special services of other countries or agents of influence. "Domination of potential aggressors in the information environment, penetration of Poland's information environment by hostile information and propaganda structures" is a potential threat to the creation of information balance (Draft Doctrine..., 2015).

The Polish Doctrine in the developed draft acquires the connotation of a directive in the statuses defining possible international conflicts. The Ukrainian Doctrine does not specify or foresee any such conflict. Note that the draft of the Polish Information Security Doctrine is still under development, despite the approval of the Polish National Security Bureau that the supposed Doctrine will be adopted by the end of 2015. As for the information security dimension, the National Security Strategy, signed by the Polish President at the submission of the Prime Minister, is "the main state document" that "establishes the conceptual basis for the organization, preparation and functioning of the national security system in times of peace, threat or war, respectively to the national interests and available conditions" (National Security Strategy, 2020).

Aspects of information security and information culture are closely related to the social responsibility of journalists. Contemporary journalism studies emphasize the weight of journalists as key facilitators within the information security framework (Bokša, 2019; Johnson, 2021; Ojala *et al.*, 2018; Seib, 2021). Broadly speaking, "Social responsibility is an ethical framework indicating that a person should cooperate with other people and organizations for the good of the society that will inherit the world left behind by that person" (Jensen, 2006).

Along with the spread of modern democratic ideals, the social responsibility theory of the media has become the norm. This theory inspires the media to self-control for the good

[1] See the legal analysis on Ukraine's information security Doctrine prepared by Professor Katrin Nyman-Metcalf, an independent legal and communications expert, on behalf of the Office of the OSCE Representative on Freedom of the Media, July 2015.

of society. But the question is, how do media practitioners and journalists adhere to this theory? Some researchers consider the social responsibility theory of journalism, framing it within an understanding of "peace journalism" aimed at examining the root causes of conflict to enable society to consider and evaluate nonviolent responses to conflict (Lynch & McGoldrick, 2005, p. 6). Still others define social responsibility as understanding journalistic behavior in the field and honesty in reporting practices (Townend *et al.*, 2016).

4. The results of the Ukrainian and Polish journalists' and editors' survey

The Ukrainian respondents who answered the questionnaire (n =24) are represented by journalists (n =16), editors (n =7) and special correspondents (n =1) and have varying levels of media experience: less than two years (n=7), two to five years (n=10), over five years (n=7). Respondents represent the following national media: *Ukrainska Pravda* (electronic media outlet, n=2), *Sohodni* (electronic and print media outlet, n=2), *1+1* (TV channel, n=2), *24 kanal* (TV channel, n=1), *BBC News Ukraina* (electronic media outlet, branch of the British broadcaster, n=1), *Deutsche Welle Ukraina* (electronic media outlet, branch of the German broadcaster, n=1), *Inter* (TV channel, n=1), *Apostrof* (electronic media outlet, n=1), *Vechirnii Kyiv* (electronic media outlet, n=1) , *Gordon* (electronic media outlet, n =1), *Detector Media* (electronic media outlet, n =1) , *Dzerkalo tyzhnia* (electronic media outlet, n =1) , *Espreso TV* (TV channel, n=1) , *Korespondent* (electronic media outlet, n=1), *Novoe vremia* (electronic and print media outlet, n=2), *RBK Ukraine* (electronic media outlet, n =1), *Strana* (electronic media outlet, n=2), *UNIAN* (state news agency, n=1), *Ukraina Moloda* (electronic and print media outlet, n =1). In general, the respondents represent the majority of national media, which are included in the rating "50 most visited media in Ukraine" (based on the Gemius and TNS rankings) and have different ownership structures. The majority of the media are private. Among them are traditionally balanced publications (e.g. *Ukrainska Pravda, Dzerkalo tyzhnia*), pro-government (e.g. *1+1*), opposition (e.g. *Inter*) and representatives of foreign broadcasters (*DW, BBC*). Such an extensive structure of presented media allows us to include opinions of a wide range of journalists and editors in the analysis.

For the survey of Ukrainian journalists and editors 9 questions-scales were developed, concerning the information security space of Ukraine, the Information Security Doctrine and interaction of journalists and editors within the information security strategy. The tau-equivalent reliability coefficient for the Ukrainian respondents' survey is 0.749.

The survey results showed that most of respondents are not familiar with the text of the Information Security Doctrine of Ukraine, which includes key provisions to protect the information space of the country and information security. This may indicate a low level of information culture of Ukrainian journalists and editors, their lack of familiarity with the documents regulating work in the information sphere. On a scale from 1 to 5 (where 1 means "not completely familiar with the text of the Information Security Doctrine") only 6 respondents chose "4" and "5" (Q1, <x> 2.50, α =0.69).

However, the majority of respondents are aware of the threats of the information space and believe that it is important to regularly update (through changes in the global political, economic, information landscape) state documents related to information security (points "4" and "5" on the scale were selected by 17 respondents, point "1" – 0). Journalists representing Ukraine foreign broadcasters and TV channels representatives ranked the highest on this scale (Q2, <x> 3.96, α = 0.70). In their journalistic activities, the respondents either do not refer at all (points 1 and 2, n = 20) or only rarely (point 3, n = 4) to the provisions of the state documents related to the information security sphere (Q3, <x> 1.71, α = 0.69). This can once again serve as a confirmation of the low information culture of some Ukrainian journalists (we should not forget that such results were obtained in a country where there is a military conflict and, at the time of the survey, there was a threat of full-scale war, which, unfortunately, came true).

In the evaluation of the scale, "Do you consider state documents concerning information security to be an element of pressure on information freedom? (from 1 – is not an instrument of pressure at all, to 5 – is an instrument of pressure)" the respondents' opinions slightly differed (Q4, <x> 2.96, α =0.74). Most of the answers (n =16) are items "2" and "3," that is, in general, the respondents do not think that the existing state documents in the sphere of information security have any influence on the full-scale informing or somehow limit the surveyed journalists or editors in their activity. However, a few respondents (n=2) chose point "5," which may indicate their belief in the functioning of such documents as an instrument of pressure, but does not give us an understanding of how such pressure is exercised.

Most of the interviewed Ukrainian journalists and editors wanted to participate in developing state documents on information security (Q5, <x> 4.25, α =0.72). A significant number of respondents are convinced that the position of the media owner influences the journalists' compliance with the provisions of the state documents on information security, which may indicate internal editorial pressure on media workers (Q6, <x> 3.33, α =0.78). It is known that oligarchs own numerous media outlets in Ukraine. This can be a severe obstacle to responsible and balanced reporting. In addition, the respondents consider inefficient the tools existing in the country to combat the information aggression (Q7, <x> 2.75, α =0.74); for the majority of respondents it is important to personally participate in the updating of documents (strategies, doctrines) related to the information security of the country (Q8, <x> 3.58, α =0.78); most respondents consider it important to sign a separate document forming the principles of social responsibility of journalists under information threats (Q9, <x> 4.0, α = 0.67).

Eight respondents expressed their thoughts in the open-ended question. Three respondents expressed the need to conclude a national standard of journalist's social responsibility (respondents 4, 8, 23); some respondents suggested gathering an expert council of journalists, politicians, lawyers, researchers to develop a unified document (23), or "borrowing practices from advanced countries" (for example, Israel, respondent 8). Respondent 21 expressed a reservation that "social responsibility of a journalist" can be a veiled term for censorship, but did not argue that "in some cases" developing such principles might be necessary; respondent 22 expressed the following: "Universal rules should be developed for journalists covering military actions as well as those working in the information war process, but they should be in the form of ethical guidelines." Respondents 1 and 7 said that existing documents on information security should be updated, and respondent 10 proposed that the focus should be on media literacy.

Polish survey respondents (n=22) are represented by journalists (n=12), editors (n=8), presenters (n=1) and analysts (n=1) and have a variety of media experience – less than two years (n=4), two to five years (n=10), over five years (n=8). Respondents represent the following national media: *Dziennik Gazeta Prawna* (printed and electronic edition, n=1), *Gazeta Polska* (electronic and printed edition, n=1), *Gazeta Wyborcza* (electronic and printed edition, n=2), *Interia* (electronic media outlet, n=1), *Nasz Dziennik* (printed and electronic edition, n=1), *Newsweek Polska* (printed and electronic edition, n=1), *Onet* (electronic media outlet, n=1), *Polsat News* (electronic media outlet, in the structure of the broadcaster *Telewizja Polsat*, n=1), *Polityka* (printed and electronic edition, n=1), *RMF FM* (radio, n=2), *Rzeczpospolita* (printed and electronic edition, n=1), *Super Express* (printed and electronic edition, n=2), *TVN 24* (TV channel, part of *TVN Media Group*, n=2), *Wirtualna Polska* (electronic media outlet, n=1), *TVP* (TV channel, n=1), *Wprost* (electronic media outlet, n=3). The respondents represent 16 national media outlets, 12 of which are among the most cited Polish media (IMM, 2020) and have different ownership structures. Interestingly, the respondents represent both "traditionally" opposition media (e.g. *Gazeta Wyborzca*) and pro-government (*TVP*), as well as, for example, the interests of the Catholic Church (*Nasz Dziennik*).

The overall tau-equivalent reliability result for the Polish respondents' survey was 0.78. In general, the analysis of the Polish respondents' answers allows us to conclude that the surveyed Polish journalists and editors are not aware of the principles of information security included in the National Security Strategy (Q1, <x> 2.82 of 5, α =0.70). Only one respondent answered that he/she was familiar with the information security part of the Strategy in detail (7). The situation is better with the National Security Doctrine (Q2, <x>3.41, α =0.72). The majority of Polish respondents believe that it is important to regularly update (due to changes in the global political, economic, informational landscape) the state documents concerning the country's information security (items "4" and "5" on the scale selected by 18 respondents, items "1" and "2" – 0). Moreover, there are no correlations similar to the Ukrainian ones – representatives of different media types assessed the importance of regular document updates equally highly (Q3, <x> 4.09, α = 0.75). However, in the process of their work, Polish journalists and editors, as well as Ukrainian ones, almost do not refer to the provisions mentioned above (Q4, <x> 2.41, α =0.70), which may indicate the lack of authority of Polish information security provisions.

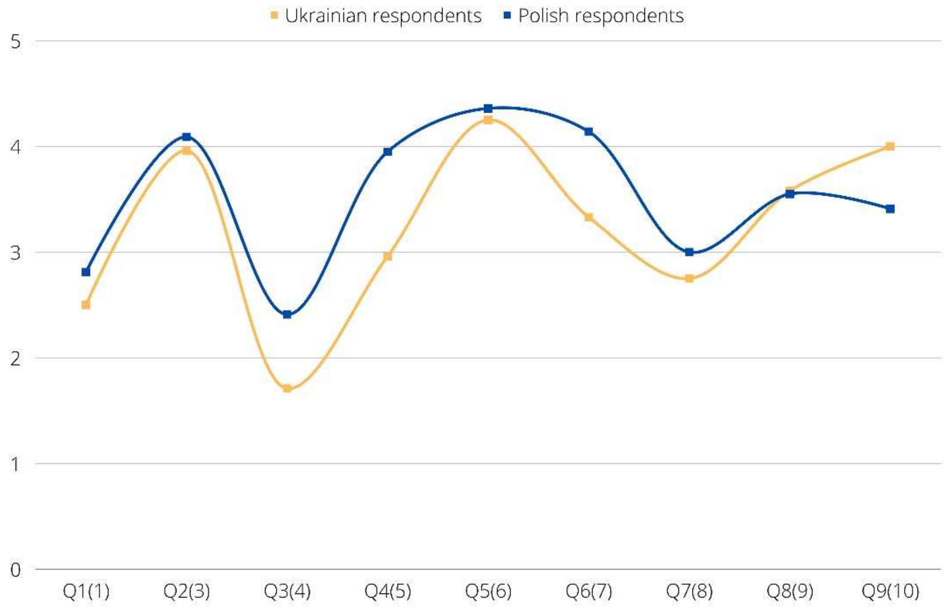
Polish journalists and editors surveyed consider the country's information policy underdeveloped. This is evidenced by the respondents' answers to the question "How effective (as a tool for combating information aggression) do you consider state documents concerning information security? (1 – not effective at all, 5 – very effective) " (Q8, <x> 3.0, α =0.82). Particular participation in the development of documents and projects related to information security, in general, is important for Polish respondents (Q9, <x> 3.55, α =0.70). Most Polish respondents also agree that the position of the media owner influences journalists' and editors' understanding and observance of state information security principles (Q7, <x> 4.14, α =0.79). Regarding the formation of individual principles of a journalist's social responsibility, the opinions of Polish respondents differed, but the majority supports such an idea (Q10, <x> 3.41, α=0.80).

Additionally, Polish respondents noted that the formation of any principles in information security should be the subject of public discussion (if it is not a period of war, respondent 1). There were also the following opinions: "I think that in our convergent times the safety of information space should be regulated, so it would be interesting to participate in a discussion involving journalists, authorities and the public" (respondent 2); "I think the social responsibility of journalism is a significant factor, because in our times of information wars it is very important to stick to the concepts of information culture and protection of strategic information from encroachment of other states" (respondent 6); "I think the social responsibility of journalism is very important, because in our times it is very essential to follow the concepts of information culture and protection of strategic information from encroachment of other states" (respondent 7). (Respondent 6); "I think we do not need a separate document. We have enough acts regulating these issues, as well as journalistic ethics" (Respondent 12); "Look at Lex TVN"[2] (Respondent 13).

Figure 2 shows the answers of both groups (n = 46) for the same scale questions for Ukrainian and Polish respondents (there are 9 such questions). Legend: Q2(3), where 2 is the ordinal number of the survey question for the Ukrainian respondents, and 3 for the Polish respondents. The scale assumed the following values: 1 – minimum, 5 – maximum.

[2] Lex TVN is a law prohibiting capital from outside the European Economic Area from owning a controlling stake in Polish media. Representatives of various media argue that these rules are a kind of attack on TV and radio stations. TVN has been trying to extend its broadcasting license for TVN 24 since February 2020, while KRRiT (the National Broadcasting Council of Poland) has been postponing the decision (it adopted it in September 2021), although previous decisions on the channel were taken much faster.

Figure 1. Results of respondents' answers to questions-scales.



Source: Survey results.

5. Conclusions

Immediately after the start of Russian aggression in Ukraine and the annexation of Crimea, both Ukraine and Poland attempted to improve information security, and both countries' official documents referred to Russia as the aggressor country. Despite this, Poland has never officially enacted an information security doctrine, and the Ukrainian doctrine requires a comprehensive update of information legislation to function effectively. Poland has developed a model of information defense – the draft Doctrine of Information Security clearly defines internal (national) and external (international) scale threats. Polish researchers try to develop and activate information security models by international reality (Liedel, 2015). Therefore, the draft doctrine introduces the concept of "hybrid warfare," and identifies threats related to "imperfect functioning of society." The Ukrainian doctrine is more susceptible to demagogy, does not provide specific methods of combating information threats, and does not provide ways to determine their effectiveness. The Polish doctrine remains in draft status, while the Ukrainian doctrine, following the decision of the National Security and Defense Council of September 14, 2020, will be updated.

The survey of journalists and editors of Polish and Ukrainian national media allows understanding how certain representatives of the fourth estate of both countries are familiar with the information legislation and how effective they consider it as a method of combating the growing information aggression. In general, the answers of journalists and editors of both countries correlate in the aspects of "how often in your journalistic activities have you referred to the provisions of state documents related to the sphere of information security" (not or not often) and regarding the effectiveness of state documents regulating the sphere of information security –not effective or to a certain extent effective. Opinions differ whether the media owner's position influences journalists' compliance with the provisions of state documents in the field of information security (5 Polish respondents indicated that it has a significant impact, while among Ukrainian respondents, this option was chosen by 1 respondent). The majority of Polish and Ukrainian respondents believe that the existing state documents in the sphere of information security are not very effective in the fight against information aggression. In general, the analysis of the answers of Polish respondents suggests that Polish journalists and editors surveyed are not aware of the principles of information security included in the National Security Strategy. The majority of Polish respondents, as well as Ukrainian respondents, believe that it is important to regularly update (due to changes in the global political, economic and information landscape) state documents concerning the country's information security.

However, in the course of their work, Polish journalists, as well as Ukrainian journalists, almost do not refer to the above provisions (for both countries <x> 2.06, α=0.70), which may indicate the lack of authority of the provisions on information security of both countries. The insufficient development of the countries' information policy can also be evidenced by the respondents' answers to the question, "How effective (as a tool to combat information aggression) do you consider the state documents related to information security? " (for both countries, <x> 2.9, α=0.78). Particular participation in the development of documents and projects in the field of information security in general is significant to respondents (for both countries, <x> 3.57, α=0.74). Most respondents would agree to join the development of state documents in the sphere of information security, which could be important to consider the balance of opinions and positions, particularly representatives of the journalistic environment.

As a continuation of our study, it would be interesting to conduct a similar survey after the beginning of Russia's full-scale war against Ukraine. In Ukraine, wartime rules came into effect, so journalists' attitudes toward the documents regulating the information space, as well as social responsibility issues, might have changed. As for Polish journalists, there is also an opportunity to update the data in the new survey, as the information agenda has changed.

We would like to thank all the respondents (journalists, editors, content analysts, and presenters) of Ukrainian and Polish media outlets who responded to the questionnaire and joined the discussion. We would also like to thank the Armed Forces of Ukraine for providing security to perform this work. This work has become possible only because resilience and courage of the Ukrainian Army.

References

Bieliszczuk, B., Ciastoń, S., Łysek, W., Niedzielski, R., Rodzik, S. & Światłowski, B. (2014). *Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej – wybrane zagadnienia* [White Paper on the Polish National Security – selected issues]. https://www.doi.org/10.12797/Poliarchia.02.2014.03.07

Bokša, M. (2019). Russian Information Warfare in Central and Eastern Europe: Strategies, Impact, Countermeasures. *German Marshall Fund of the United States*. Retrieved from https://www.jstor.org/stable/resrep21238

Dahmen, N. S., Abdenour, J., McIntyre, K. & Noga-Styron, K. E. (2018). Covering mass shootings. *Journalism Practice*, *12*(4), 456-476. https://www.doi.org/10.1080/17512786.2017.1326832

Decree of the President of Ukraine no. 47/2017 on the decision of the National Security and Defense Council of Ukraine of December 29, 2016 on the Doctrine of Information Security of Ukraine. Retrieved from https://www.president.gov.ua/documents/472017-21374

Draft Doctrine of Information Security of the Republic of Poland (2015). Retrieved from https://www.bbn.gov.pl/ftp/dok/01/Projekt_Doktryny_Bezpieczenstwa_Informacyjnego_RP.pdf

Golovchenko, Y., Hartmann, M. & Adler-Nissen, R. (2018). State, media and civil society in the information warfare over Ukraine: citizen curators of digital disinformation. *International Affairs*, *94*(5), 975-994. https://www.doi.org/10.1093/ia/iiy148

Hanitzsch, T., Anikina, M., Berganza, R., Cangoz, I., Coman, M., Hamada, B., ... & Yuen, K. W. (2010). Modeling perceived influences on journalism: Evidence from a cross-national survey of journalists. *Journalism & Mass Communication Quarterly*, *87*(1), 5-22. https://www.doi.org/10.1177/107769901008700101

Horbulin, Vlasiuk & Kononenko (2015). *Ukraina i Rosiia: deviatyi val chy kytaiska stina*. [Ukraine and Russia: the Ninth Wall or the Chinese Wall]. Retrieved from http://old.niss.gov.ua/content/articles/files/Gorbulin_Ukraine_08_05_pereverstka2.indd-2da77.pdf

Internal and External Situation of Ukraine in the Field of National Security (2014): Analytical Report of the National Institute for Strategic Studies to the President's Special Address to the Verkhovna Rada of Ukraine. Retrieved from https://niss.gov.ua/sites/default/files/2015-12/Dopovid_Prezudentps-0ab72.pdf

Jensen, D. (2006). *Endgame, volume 1: The problem of civilization* (Vol. 1). Seven Stories Press.

Lavrakas, P. J. (2008). *Encyclopedia of Survey Research Methods*. Thousand Oaks, CA: Sage. https://www.doi.org/10.4135/9781412963947

Legal Analysis of the Draft Concept of Information Security of Ukraine (2015). Office of the OSCE Representative on Freedom of the Media. Retrieved from https://ips.ligazakon.net/document/MU15066

Liedel, K. (2015). Zagrożenie hybrydowe. Jak zmienia się środowisko bezpieczeństwa RP [The hybrid threat. How the RP security environment is changing]. *Przegląd Bezpieczeństwa Wewnętrznego. Wydanie specjalne – Wojna hybrydowa* [Homeland Security Review. Special Edition – Hybrid War], pp .51-58. Retrieved from https://www.abw.gov.pl/pl/pbw/publikacje/przeglad-bezpieczenstwa-4/1213,Przeglad-Bezpieczenstwa-Wewnetrznego-WYDANIE-SPECJALNE.html

Liu, H.-L. & Lo, V.-H. (2018). An integrated model of workload, autonomy, burnout, job satisfaction, and turnover intention among Taiwanese reporters. *Asian Journal of Communication*, *28*(2), 153-169. https://www.doi.org/10.1080/01292986.2017.1382544

Lynch, J. & McGoldrick, A. (2005), *Peace Journalism*. Stroud, UK: Hawthorn Press.

Magda E. (2015). *Hibrydna viina: vyzhyty i peremohty* [Hybrid War: Survive and Win]. Vivat Publishing.

Menke, M., Kinnebrock, S., Kretzschmar, S., Aichberger, I., Broersma, M., Hummel, R., … & Salaverría, R. (2018). Convergence culture in European newsrooms. *Journalism Studies*, *19*(6), 881-904. https://www.doi.org/10.1080/1461670X.2016.1232175

Misko V. (2017). *Svitova hibrydna viina: ukrainskyi front:* monohrafiia/za zah. red. VP Horbulina [World Hybrid War: Ukrainian Front: Monograph / Edited by OP Gorbulin].–Kharkiv: Folio, 2017. Retrieved from https://niss.gov.ua/publikacii/monografii/svitova-gibridna-viyna-ukrainskiy-front-monografiya

Molyneux,L. & Zamith, R. (2020). Surveying journalists in the "New Normal": Considerations and recommendations. *Journalism*, *23*(1), 153-170. https://www.doi.org/10.1177/1464884920935277

National Security Bureau (2013). Biała księga bezpieczeństwa narodowego Rzeczypospolitej Polskiej [National Security White Paper of the Republic of Poland]. *National Security Bureau of Poland*. Retrieved from https://www.bbn.gov.pl/pl/informacje-o-bbn/publikacje/6815,Biala-Ksiega-Bezpieczenstwa-Narodowego-RP.html

National Security Strategy of the Republic of Poland (2020). Retrieved from https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf

Eugeniusz, N., Maciej, N. (2011). *Zarys teorii bezpieczeństwa narodowego* [Theoretical outline of national security]. Warszawa*:* Difin [Warsaw: Difin]. Retrieved from https://ksiegarnia.difin.pl/zarys-teorii-bezpieczenstwa-narodowego-wydanie-2

Ojala, M., Pantti, M. & Kangas, J. (2018). Professional role enactment amid information warfare: War correspondents tweeting on the Ukraine conflict. *Journalism*, *19*(3), 297-313. https://www.doi.org/10.1177/1464884916671158

Parakhonskyi B., Yavorska H. (2015). *Zovnishnia polityka Ukrainy v umovakh kryzy mizhnarodnoho bezpekovoho seredovyshcha: analitychna dopovid* [Ukraine's foreign policy in a crisis of international security: analytical report]. Retrieved from https://niss.gov.ua/sites/default/files/2015-11/Kruza_Yavor.indd-36e36.pdf

Pocheptsov, G. (2016). *Smysly i viiny: Ukraina i Rosiia v informatsiinii i smyslovii viinakh.* [Meanings and War: Ukraine and Russia in the Information and Meaning Wars]. Kyiv: Kyievo-Mohylianska akademiia (Kiev: Kiev-Mohyla Academy).

Razumkov Center (2019). Viina na Donbasi: realii i perspektyvy vrehuliuvannia [The War in Donbas: Realities and Prospects for Settlement]. *Razumkov Center.* Retrieved from https://razumkov.org.ua/uploads/article/2019_Donbas.pdf

Seib, P. (2021). *Information at War: Journalism, Disinformation, and Modern Warfare.* Medford, MA: Polity Press.

Semenihin, I. (2018). Legal doctrine: aspects of understanding. *Problems of Legality*, *141*, 8-21. https://www.doi.org/10.21564/2414-990x.141.130708

Shemchuk, V. (2019). Informatsiina bezpeka ta informatsiina oborona v konteksti rozvytku vitchyznianoi doktryny y zakonodavchoi osnovy [Information security and information defense in the context of domestic doctrine and legislative framework development]. *Vcheni zapysky Tavriiskoho natsionalnoho universytetu imeni VI Vernadskoho* [Scientific notes of V. I. Vernadsky Taurida National University], *4*, 31-37. https://www.doi.org/10.32838/1606-3716/2019.4/06

Sielezin, J. R. (2020). Post-prawda jako element polityki historycznej Rosji wobec Polski– kontekst międzynarodowy [Post-truth as an element of Russia's historical policy towards Poland - the international context]. *Facta Simonidis*, *13*(1), 45-59. Retrieved from https://www.ceeol.com/search/article-detail?id=912309

Strategic National Security Review (2012). Retrieved from https://www.bbn.gov.pl/pl/prace-biura/glowne-inicjatywy/lata-2010-2015/strategiczny-przeglad-b

Taber, K.S. (2018). The Use of Cronbach's Alpha When Developing and Reporting Research Instruments in Science Education. *Res Sci Educ* 48, 1273–1296. https://www.doi.org/10.1007/s11165-016-9602-2

The Cybersecurity Strategy of the Republic of Poland for 2019-2024 (2019). Retrieved from https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2019-2024

Townend, J., Muller, D. & Keeble, R. L. (2016). Beyond clickbait and commerce: The ethics, possibilities and challenges of not-for-profit media. *Ethical Space*, *13*(2-3), 1-116. Retrieved from https://sas-space.sas.ac.uk/6359/

Transcript of the meeting of the Verkhovna Rada Committee on Freedom of Speech and Information Policy of January 18, 2017. Retrieved from http://komsvobslova.rada.gov.ua/documents/zasid/73189.html

Visser, P. S., Krosnick, J. A., Marquette, J. & Curtin, M. (1996). Mail Surveys for Election Forecasting? An Evaluation of the Colombia Dispatch Poll. *Public Opinion Quarterly*, *60*(2), 181–227. https://www.doi.org/10.1086/297748

Vlasiuk O. (2016). *Natsionalna bezpeka Ukrainy: evoliutsiia problem vnutrishnoi polityky: vybrani naukovi pratsi* [National Security of Ukraine: Evolution of Problems of Internal Policies: Selected Research Works]. Retrieved from https://niss.gov.ua/sites/default/files/2017-01/Vlasuk-fin-99d56.pdf

Zolotar, O. O., Zaitsev, M. M., Topolnitskyi, V. V., Bieliakov, K. I. & Koropatnik, I. M. (2021). Prospects and current status of defense information security in Ukraine. *Linguistics and Culture Review*, *5*(S3), 513-524. https://www.doi.org/10.21744/lingcure.v5nS3.1545

Appendix 1. List of scale questions that respondents answered, and the average result of the values obtained (<x>)

Scale question	**(<x>) (Polish respondents)**	**(<x>) (Ukrainian respondents)**
How familiar are you with the text of the Doctrine of Information Security of Ukraine (for Ukrainians) / Poland (for Poles)?(from 1 - not familiar at all to 5 - completely familiar)	**2.81**	**2.50**
How familiar are you with the text of the Polish National Security Strategy? (from 1 - not familiar with it at all, to 5 - fully familiar with it)	**3.41**	
Do you think it is important to regularly update (due to changes in the global political, economic, information landscape) government documents related to information security? (from 1 - I don't think it's important to 5 - I think it's very important)	**4.09**	**3.96**
How often in your journalistic/editorial work do you refer to the provisions of government documents related to information security? (from 1 - do not refer at all to 5 - do refer often).	**2.41**	**1.71**
Do you think that government documents concerning information security are an instrument of pressure on information freedom? (from 1 - not a pressure instrument at all, to 5 - definitely a pressure instrument)	**3.95**	**2.96**
In your opinion, how important is it for representatives of the national media to participate in the development of government documents on information security? (from 1 - not important at all, to 5 - very important)	**4.36**	**4.25**
In your opinion, to what extent does the media owner's position influence journalists' compliance with the provisions of state documents on information security? (1 - does not influence at all, 5 - significantly influences).	**4.14**	**3.33**
How effective (as a tool for combating information aggression) do you consider government documents related to information security? (1 - not effective at all, 5 - very effective).	**3.00**	**2.75**
How important is it for you to personally participate in the updating of documents (strategies, doctrines) that concern the information security of your country? (from 1 - not important at all, to 5 - very important)	**3.55**	**3.58**
How important do you think it is to conclude a separate document forming the principles of social responsibility of journalists under information threat? (1 - not important at all, 5 - very important)	**3.41**	**4.00**