Information Security Policy

Conditions, Threats and Implementation in the International Environment

EDITED BY
PIOTR BAJOR

INFORMATION SECURITY POLICY

INFORMATION SECURITY POLICY

Conditions, Threats and Implementation in the International Environment

edited by

PIOTR BAJOR

WYDAWNICTWO
KSIĘGARNIA AKADEMICKA
Sp. z o.o. Kraków

Kraków 2022

Piotr Bajor
Jagiellonian University in Kraków, Poland
iD https://orcid.org/0000-0003-2569-2552
✉ piotr.bajor@uj.edu.pl

Review: Marek Delong

Language editor:
Cover design: Marta Jaszczuk

ISBN 978-83-8138-826-9 (print)
ISBN 978-83-8138-827-6 (PDF)
https://doi.org/10.12797/9788381388276

The opinions expressed in this publication are those of the authors and do not reflect the views of the official positions of the Ministry of Foreign Affairs of the Republic of Poland.

Ministry
of Foreign Affairs
Republic of Poland

Public task financed by the Ministry of Foreign Affairs of the Republic of Poland within the grant competition “Public Diplomacy 2022”.

centrum badań nad
współczesnym
środowiskiem
bezpieczeństwa

The project was implemented by the Foundation Center for Research on the Contemporary Security Environment, in cooperation with a research team from the Jagiellonian University in Kraków.

KSIĘGARNIA AKADEMICKA PUBLISHING
ul. św. Anny 6, 31-008 Kraków
tel.: 12 421-13-87; 12 431-27-43
e-mail: publishing@akademicka.pl
https://akademicka.pl

Table of contents

INFORMATION SECURITY POLICY:
Conditions, Threats and Implementation
in the International Environment, pp. 99–121
https://doi.org/10.12797/9788381388276.06

Piotr Bajor
Jagiellonian University in Kraków

Information Security Policy of Ukraine – Assumptions and Effectiveness

Abstract: The paper presents the results of research on Ukraine's information security, analysed from the perspective of its tenets, implementation and effectiveness. In this regard, the paper discusses aspects related to the development of conceptual tenets and preparation of a security strategy, as well as sectoral strategies and doctrines of information security and cybersecurity. The paper also contains an analysis of the institutional dimension of information security and actions taken by Ukraine in connection with the Russian aggression in terms of strategic communication and cybersecurity.

Keywords: security policy, information policy, cybersecurity

Introduction

Information security is becoming an increasingly important concept in the modern world and is among the key categories of national security interests. The technological revolution, digitisation and computerisation of states, as well as the dynamic development of mass media and the rising role and importance of social media, have affected the evolution and significance of these processes in the context of security. As a result, we now live in a world where aspects related to information, both in terms of content and technology, play a key role in the functioning and security of states. These processes are important during peace but become even more crucial in times of danger, conflict and war. This is of particular significance given the current situation related to Russia's aggression against Ukraine. The purpose of this paper is, therefore, to present the results of research into Ukraine's information security policy, including its legal aspects, doctrinal assumptions and implementation during peacetime and during the war that began in early 2022.

As part of the research process, a hypothesis was formulated that Ukraine has increased its capabilities in terms of information resilience and the effectiveness of information security policy through implementing legislative, legal, organisational and technical means in recent years as a result of threats to its information security during this time. The research was based on the content analysis method, comparative method and historical method.

Conceptual premises of information security

Concepts found in the normative document titled "Ukraine's information security strategy" (dated 28 December 2021) were used for this paper in terms of its definitional and conceptual aspects. According to the strategy, information security is "an integral part of Ukraine's national security, a way of ensuring the sovereignty of the state, its territorial integrity, democratic and constitutional governance, other vital interests of individuals, the society and the state – which guarantee constitutional rights and civil liberties, including the right to gather, store, use and distribute information and access reliable and objective information".[1] The above definition is complemented by the clarification of the concept of an "information threat", which is considered as "potential and actual phenomena, factors and tendencies related to the impact of information on the individual, the society and the state, which are present in the information sphere and whose purpose is to exert a negative influence aimed at preventing or hampering the achievement and pursuit of national interests".[2] Based on the above aspects and definitions, we can state that the information security of Ukraine has been given

[1] "Указ Президента України №685/2021 Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»", *President of Ukraine: Official website*, [on-line:] https://www.president.gov.ua/documents/6852021-41069 (27.09.2022). See also: О.Д. Довгань, Т.Ю. Ткачук, "Система інформаційної безпеки України: онтологічні виміри", *Інформація і право*], vol. 1, no. 24 (2018), pp. 90–97.

[2] "Указ Президента України №685/2021…"

a broad definition that accounts for elements of a social, political, economic, technical and infrastructural nature.

Ukraine's information security strategy

The above definition of Ukraine's information security is the product of many years of experience in this area, gained in recent years in which Ukraine was facing multiple challenges in this sphere due to the ongoing hybrid war.[3] The annexation of Crimea in 2014 and the subsequent conflict in the eastern oblasts of Ukraine, related to the activity of separatist entities supported by Russia, constituted a breakthrough in how Ukraine perceived security information and the threat posed by Russia in this area.[4] The evolution of threats in the sphere of information security and the need to take adequate action in response to them formed the basis of Ukraine's Strategy of National Security, adopted on 26 May 2015,[5] as well as Ukraine's Information Security (dated 25 February 2017).[6]

The hybrid war that raged in subsequent years confirmed the threats to information security were constantly rising. Ukraine reacted to these challenges on an ongoing basis and attempted to combat the threats in this area effectively. Experience from the confrontations that took place as part of the information war, and the resulting adaptation of the national security system in this sphere, also became the basis for a systemic analysis and update of strategic national security documents. Work aimed at

[3] Т. Жовтенко, "Гібридна війна: анатомія інструментарію й перемоги", *Democratic Initiatives*, 3.11.2022, [on-line:] https://dif.org.ua/article/gibridna-viyna-anatomiya-instrumentariyu-y-peremogi (27.09.2022); Т.О. Ісакова, "Пропаганда спрямована на розпалювання національної та міжнаціональної ворожнечі: проблеми визначення та протидії", *Аналітична записка*, no. 2, Серія «Інформаційні стратегії», NISS, 2.03.2015, [on-line:] https://niss.gov.ua/doslidzhennya/informaciyni-strategii/propaganda-spryamovana-na-rozpalyuvannya-nacionalnoi-ta (27.09.2022).

[4] See: M. L. Jaitner, "Russian Information Warfare: Lessons from Ukraine", in K. Geers (ed.), *Cyber War in Perspective: Russian Aggression against Ukraine*, NATO CCD COE Publications, Tallinn 2015, pp. 91–93.

[5] "Указ Президента України Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року 'Про Стратегію національної безпеки України'", *Verkhovna Rada of Ukraine*, [on-line:] https://zakon.rada.gov.ua/laws/show/392/2020#Text (27.09.2022).

[6] "Указ Президента України №47/2017 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»", *President of Ukraine: Official website*, [on-line:] https://www.president.gov.ua/documents/472017-21374 (27.09.2022). See also: Т. Попова, "Що означає «Доктрина інформаційної безпеки України»?", *Radio Svoboda*, 27.02.2017, [on-line:] https://www.radiosvoboda.org/a/28337376.html (27.09.2022); "Доктрина інформаційної безпеки України – це лише декларація – експерти", *Radio Svoboda*, 27.02.2017, [on-line:] https://www.radiosvoboda.org/a/28336852.html (27.09.2022).

preparing new versions of these documents, taking into account the changed terms on which the hybrid war was being waged and rising threats in the information security area were constantly ongoing.[7]

Ukraine's new National Security Strategy was ultimately adopted on 14 September 2020. The document concerned broadly defined state security while accounting for challenges and threats in the sphere of information security. As far as this aspect was concerned, it was noted that given the circumstances, scale and importance of the information sector to national security, a special document concerning the specific area of information security had to be developed.[8] Work on the document continued in subsequent months, and ultimately on 28 December 2021, President Volodymyr Zelenskyy approved the *Strategy of Information Security of Ukraine.*[9]

The document points to the most critical aspects related to threats and challenges facing Ukraine in the sphere of information security. Guaranteeing Ukraine's security in this area was considered one of the state's most important tasks, given the severity of threats in this sphere, particularly in the context of the danger posed by Russia. The document stressed that Russia was pursuing a very aggressive policy in the sphere of information in respect of Ukraine, aimed at undermining the sovereignty and territorial integrity of the Ukrainian state. The objective of Ukraine's activity in the area of information security is to neutralise this aggressive policy pursued by the Russian Federation, as well as special operations related to information policy, aimed at weakening and undermining Ukraine's sovereignty and territorial integrity.[10]

[7] See also: "Аналіз Стратегії інформаційної безпеки в порівнянні з чинною Доктриною інформаційної безпеки", *Institute of Mass Information*, 29.04.2021, [on-line:] https://imi.org.ua/monitorings/analiz-strategiyi-informatsijnoyi-bezpeky-v-porivnyanni-z-chynnoyu-doktrynoyu-informatsijnoyi-i38852 (27.09.2022).

[8] "Указ Президента України Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року 'Про Стратегію національної безпеки України'", *Verkhovna Rada of Ukraine*, [on-line:] https://zakon.rada.gov.ua/laws/show/392/2020#Text (27.09.2022).

[9] "Указ Президента України №685/2021…"; See also: "Стратегію інформаційної безпеки-2025 прийнято: що зміниться у сфері цифрових прав?", *Digital Security Lab*, 18.01.2022 [on-line:] https://dslua.org/publications/stratehiiu-informatsiynoi-bezpeky-2025-pryyniato-shcho-zminytsia-u-sferi-tsyfrovykh-prav/ (27.09.2022).

[10] "Указ Президента України №685/2021…"; "7 стратегічних цілей інформаційної безпеки України", *LexInform*, [on-line:] https://lexinform.com.ua/zakonodavstvo/7-strategichnyh-tsilej-informatsijnoyi-bezpeky-ukrayiny/ (27.09.2022).

Analysis of threats in the area of information security

The evolution of considerations related to information security – both internationally and internally, as well as the perception of threats facing Ukraine – determined the division of dangers in this area. Taking into account the major aspects affecting key security information processes, the four following categories were considered the most important threats in the area of information:

- increase in the number of global disinformation campaigns;
- Russia's information policy (in respect of both Ukraine and other democratic states);
- an increase of the importance of social media in the context of impact factors and tools in the information space;
- insufficient level of development of competencies and skills in the context of the rapid development of information and digital technologies.[11]

Regarding threats in this international sphere, Ukraine treats information security as a challenge that constitutes a substantial global threat. Ongoing global disinformation campaigns pursued by authoritarian governments and radical groups aim to broadly impact, distort and manipulate social awareness. In the opinion of Ukrainian authorities, such actions are implemented by authoritarian countries on a widespread basis, which affects the democratic development of states and, from a broader perspective, international stability.[12]

In the context of the above challenges, the information policy and actions of the Russian Federation were considered a threat not only to the Ukrainian state, but to other democratic states as well. Based on experiences from activities pursued in recent years in respect of Ukraine, it was then found that Russia uses its special services and other dedicated structures to perform targeted operations and attacks against individual states. These attacks aim to influence internal public opinion and sow internal divisions among societies. The document, therefore, states that it is of paramount importance to counteract these operations and implement monitoring activities aimed at intercepting and eradicating intentional messages and disinformation.[13]

The use of social media is part of these activities. Their significance and use have risen sharply in recent years, which was determined by factors including globalisation

[11] "Указ Президента України №685/2021…"; В. Новицький, "Стратегічні засади забезпечення інформаційної безпеки в сучасних умовах", *Інформація і право*, vol. 1, no. 40 (2022), pp. 114–115.

[12] "Указ Президента України №685/2021…"

[13] *Ibidem*; "Президент увів у дію рішення РНБО про Стратегію інформаційної безпеки", *Ukrinform*, 28.12.2021, [on-line:] https://www.ukrinform.ua/rubric-polytics/3376906-prezident-uviv-u-diu-risenna-rnbo-pro-strategiu-informacijnoi-bezpeki.html (27.09.2022).

and the COVID-19 pandemic. The specific nature of social media results in a significant increase in its importance for the social and political situation – both in terms of internal affairs of specific states as well as in the general context of global processes. Given the above, social media are a crucial tool in the modern security environment from the point of view of information and have extremely important effects from a security perspective.[14]

From the point of view of Ukraine's stance on threats, the above processes are correlated with the public perception of content and messages being communicated. Given the specific nature of contemporary media in terms of their availability, freedom and ease of conveying information and general accessibility, the strategy underlined the reduced social resilience to the content and narrative being communicated. Therefore, these considerations and processes constitute a significant threat given their potential for influencing and manipulating the entire society. They can significantly improve the effectiveness of information and psychological campaigns and the success of propaganda and disinformation and, as such, poses a significant threat to information security.[15]

Internal dimension of threats in the information sphere

Given the list of threats in the sphere of information, analysing related processes and factors is of crucial importance from the perspective of Ukraine's circumstances and interests. The situation in this regard is affected by both systemic considerations and the heritage of Ukraine's social and political transformation processes and new phenomena and developments in this area. Due to this, Ukraine has delineated several key threats to national security in the sphere of information, which include the following processes:

- the information-related impact of the Russian Federation as an aggressor state on the Ukrainian people;
- Russia's domination in terms of information as an aggressor state in temporarily occupied areas of Ukraine;
- limited possibilities of reacting to and counteracting disinformation campaigns;
- the lack of an effective strategic communication system;
- imperfection in the regulation of relations in the sphere of information and protection of professional activities of journalists;

[14] "Указ Президента України №685/2021…"

[15] *Ibidem.*

- attempts to manipulate social consciousness in terms of European integration processes and Ukraine's Euro-Atlantic integration;
- limited access to information on the local level;
- insufficient level of information culture in society – in particular, in terms of susceptibility to manipulation and information influence.[16]

Ukraine pointed to information security on a national scale as one of the most important aspects of threats to its sovereignty and identity as a state. The Russian Federation was once again found to be the source of key threats in this sphere. Ukraine stressed that Russian intelligence services had been coordinating operations against Ukraine for some time, aimed at undermining its stability and internal security. The objective of these actions is to weaken Ukraine's national interests, sow division and conflict among its society, destabilise the social and political situation, eradicate Ukrainian national identity and ultimately bring about the end of Ukraine as a sovereign state. In this context, it's worth pointing out the actions taken and the current situation in terms of information security in areas occupied by the Russian Federation. Ukraine underlined that Russia had built a new information infrastructure in Crimea and was pursuing similar activities in the eastern oblasts of Ukraine. Apart from technical aspects, freedom of speech and civil liberties were restricted, and the activities of editing teams and journalists were under close supervision and control of authorities. As a result of these actions, the people living in these areas are cut off from any information disseminated by Ukraine and have access solely to narratives and propaganda content served by Russia. This situation poses a particular threat to Ukraine in the context of the state's communication with its citizens, supporting pro-Ukrainian attitudes and providing Ukrainians with information independent of the Russian authorities.[17]

The "destructive" propaganda and disinformation activities pursued by Russia on a comprehensive and full-scale basis constitute a key threat to the internal stability and security of the Ukrainian state in these two dimensions. By analysing the above threats, the tactics of which change depending on the current situation and social and political processes, Ukraine attempts to counteract them via various methods and

[16] *Ibidem*, "Зеленський затвердив Стратегію інформаційної безпеки України", *Institute of Mass Information*, 29.12.2021, [on-line:] https://imi.org.ua/news/zelenskyj-zatverdyv-strategiyu-informatsijnoyi-bezpeky-ukrayiny-i43121 (27.09.2022).

[17] "Указ Президента України №685/2021…"; В. Новицький, *op. cit.*, pp. 114–115; See also: "Журналістика на території України в умовах гібридної війни: межі та можливості державного регулювання. Аналітична записка", *NISS* [on-line:] https://niss.gov.ua/doslidzhennya/informaciyni-strategii/zhurnalistika-na-teritorii-ukraini-v-umovakh-gibridnoi-viyni (27.09.2022).

activities. Authorities strive to adapt legal regulations and organisational solutions to the challenges facing them in this regard. However, as confirmed in the strategy, the analysis of the threats has still not led to the creation of comprehensive methods of counteracting and negating Russian "information aggression". Ukraine has, therefore, implemented further plans and undertaken actions aimed at creating an effective system of strategic communication and preventing threats in the area of information that constitute a significant danger to the state's stability and national security.[18]

Analysis of threats to internal information security shows that the situation in and functioning of the Ukrainian media market remains a significant problem in this regard. The structure of ownership and control of media by oligarch groups, limited potential for competition among media, as well as lack of independence of journalists from media owners are not conducive to the development and independence of media and affect the efficacy of actions undertaken to combat threats in the area of information security.[19]

The above is particularly true at the regional level, where media often remain dependent on local business structures and authorities. These circumstances are largely the product of the huge disproportions in the Ukraine media market. Huge disparities continue to exist between large cities and regional centres and smaller towns, where there is often a lack of information infrastructure and access to the internet. This has led to significant information exclusion of a large part of society and its dependence on local media.[20]

Of note is also that the above aspects of information policy were tied to Ukraine's foreign and security policies, aimed at becoming part of the European Union and NATO. The strategy stresses that the majority of its citizens supports these two key objectives of Ukraine's international policy. Given the strategic nature of this direction, Russia has been taking hostile action by manipulating and influencing Ukrainian citizens by disseminating untrue and stereotypical information on the EU and NATO. The purpose of this information is to destroy national consolidation and unity as to the direction of foreign and security policy and obstruct and subvert reforms being

[18] "Указ Президента України №685/2021…"; see also: "Президент затвердив Стратегію інформаційної безпеки: що передбачено", *Jurliga*, 29.12.2021, [on-line:] https://jurliga.ligazakon.net/news/208447_prezident-zatverdiv-strategyu-nformatsyno-bezpeki-shcho-peredbacheno (27.09.2022).

[19] "Указ Президента України №685/2021…"

[20] *Ibidem*; "Міжнародний досвід впровадження медіаграмотності для окремих цільових груп: можливості для України", *Niss*, 14.05.2019, [on-line:] https://niss.gov.ua/doslidzhennya/informaciyni-strategii/mizhnarodniy-dosvid-vprovadzhennya-mediagramotnosti-dly (27.09.2022).

implemented in the country in connection with its policy of integration with the EU and NATO.[21]

Strategic objectives and directions of development of information security

Based on its analysis of considerations and threats related to the information area, Ukraine set seven strategic objectives, the achievement of which was to improve the situation in the diagnosed weak points of the information system. Implementing actions in these areas would also improve the resilience of the state and increase information security.[22] Based on the *Strategy of Information Security*, the following seven strategic objectives were set:

- Strategic objective No. 1: the objective concerns counteracting propaganda and disinformation, combating special operations in the area of information pursued by a hostile state, aimed at destroying constitutional governance, weakening the sovereignty and damaging the integrity of the Ukrainian state and eradicating Ukrainian independence. In this regard, Ukraine planned implementing a system of early warning and prevention of hybrid threats with particular attention placed on counteracting disinformation, propaganda, and information operations. Plans also included creating a mechanism of counteracting disinformation related to foreign policy and security of the Ukrainian state and its ongoing policy of European and Euro-Atlantic integration aimed at deepening Ukraine's cooperation with the EU and NATO;
- Strategic objective No. 2: the objective concerned strengthening Ukrainian identity and preparing and ensuring the comprehensive development of Ukrainian culture. This factor was determined as a key aspect in the context of building identity, a basis for the consolidation of the Ukrainian society and improving the national community;
- Strategic objective No. 3: the objective concerned activities aimed at improving the level of media culture and increasing the competences of citizens in the area of information. Actions in this aspect were directed mostly at improving social awareness to build resilience against propaganda, disinformation, destructive influences and manipulations forming part of hybrid activities pursued by the aggressor state;

[21] *Ibidem*…; В. Новицький, *op. cit.*, pp. 114–115.

[22] "Зеленський затвердив Стратегію…"; В. Новицький, *op. cit.*, pp. 114–115.

- Strategic objective No. 4: the objective concerned strengthening democratic processes and guaranteeing human rights in the area of information, freedom of speech and expressing one's views, and ensuring diversity of sources and access to verified, objective and reliable information. Strengthening journalistic work and guaranteeing the safety of those practising this profession, as well as freedom and independence of action while pursuing their duties;
- Strategic objective No. 5: the objective concerned a special form of Ukraine's information policy aimed at Ukrainian citizens living in occupied territories. The objective was described as "reintegration in terms of information" with the Ukrainian media space and own Ukrainian narratives addressed to these groups of citizens. Objectives in these areas were specified on a national and international scale. On the national scale, actions involved steps aimed at reaching citizens living in occupied areas with Ukrainian messages. On the international scale, the objective was to pursue consistent actions in respect of the international community, informing and reminding it of the status of Crimea and its occupation by Russia, as well as the occupation of the eastern oblasts of Ukraine;
- Strategic objective No. 6: the objective concerned actions aimed at implementing further changes and creating an effective system of strategic communication, with a focus on the key role of coordination of actions taken by authorities and structures responsible for information policy. Actions in this area were to result in strengthening cooperation between individual authorities and enabling them to counteract propaganda and disinformation effectively. It's worth noting that actions in this regard were focused on both internal and international circumstances and processes. Their goal was to counteract false Russian messaging concerning Ukraine and improve the state's positive image in the international arena;
- Strategic objective No. 7: the objective concerned actions aimed at developing and strengthening the society in the sphere of information and improving the culture of social dialogue. An integral part of these actions was to deepen and expand the public debate, improve the position of and funding for public broadcasters, expand modern information infrastructure and develop research into the information space, with a particular focus on the impact of new forms of mass media, social media, and online content on social processes and the functioning of societies.[23]

The strategic goals set were based mainly on a diagnosis of circumstances and challenges facing Ukraine in the information sphere. They were aimed primarily at improving the effectiveness of actions in the area of information security and the state's

[23] "Указ Президента України №685/2021…"; "7 стратегічних цілей інформаційної безпеки…".

resilience against internal and external threats. The Russian aggression on Ukraine cut these preparations short. Still, many of the implemented components contributed to increased effectiveness of actions taken by Ukraine in the information sphere and its narratives in the international arena concerning messaging around the Russian attack.

Ukraine's cybersecurity

Cybersecurity is another key component of information security. From Ukraine's perspective, this sphere constitutes a very important part of national security due to frequent cyber-attacks on this country. As a result, on 15 March 2016, the then-President of Ukraine, Petro Poroshenko, adopted the first sectoral document, namely the Strategy of Cybersecurity of Ukraine.[24] After a few years, authorities decided to update the document[25] and, on 26 August 2021, President Volodymyr Zelenskyy approved the latest version of the Strategy of Cybersecurity of Ukraine.[26]

According to the document, the state's cybersecurity is one of the key priorities in Ukraine's national security system. It, therefore, stated that actions are needed in this area to improve the state's capabilities to counteract the cybernetic threats and attacks directed at Ukraine, particularly in the modern world, which has been seeing a rapid rise in the number of cyber threats, directly impacting a number of aspects of functioning and management of the country. The professional nature and nationalisation of cyberattacks are also of particular importance, which are carried out by special cybernetic units created as special forces forming part of the armed forces. As regards direct threats to Ukraine in this area, cybernetic threats were found to constitute "a possible arena of hostilities".[27]

The Russian Federation was again considered the source of Ukraine's cybernetic threats. Russia was found to be one of the greatest threats to cybersecurity, not only in

[24] "Указ Президента України №96/2016 Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»", *President of Ukraine: Official website,* [on-line:] https://www.president.gov.ua/documents/962016-19836 (27.09.2022).

[25] Д. Дубов, "Формуючи нову Стратегію кібербезпеки України: чи зможемо уникнути помилок першої спроби стратегування?", *NISS*, 27.01.2021, [on-line:] https://niss.gov.ua/doslidzhennya/informaciyna-politika/formuyuchi-novu-strategiyu-kiberbezpeki-ukraini-chi-zmozhemo (27.09.2022).

[26] "Указ Президента України №447/2021 Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»", *President of Ukraine: Official website,* [on-line:] https://www.president.gov.ua/documents/4472021-40013 (27.09.2022).

[27] *Ibidem*; "Нова Стратегія кібербезпеки України", *LexInform*, [on-line:] https://lexinform.com.ua/zakonodavstvo/nova-strategiya-kiberbezpeky-ukrayiny/ (27.09.2022).

Ukraine, but in other countries in the international arena as well, as Russia is carrying out special operations and attacks in cyberspace against the computer infrastructure of other countries, aiming to cripple them. Given the current technical considerations and processes in this area, from Ukraine's perspective, threats in the sphere of cybersecurity will continue to increase with the increase in the intensity of cyberattacks. Ukraine was particularly exposed to this threat and was planning on implementing actions aimed at improving its resilience and increasing the state's effectiveness in combating cybernetic security threats.[28]

This made it very important to determine the circumstances and specific nature of the operation of Ukraine's technological infrastructure and entire cybernetic system. Analysis in this regard was meant to ascertain the system's weak points and implement actions aimed at improving its effectiveness and resilience. Taking the above premises into account and based on the circumstances and threats present, major risk factors in the sphere of cybersecurity were found to (primarily) include Ukraine's high dependency on technological imports. Another vital consideration in this aspect was the dependency on foreign manufacturers and suppliers, as well as a lack of a system of technical supervision and control of the use of subsystems that could act as dual-use elements and generate a cyber threat. Other risk factors included the lack of modern legal regulations applicable to the dynamically changing sphere of cybersecurity and related threats, as well as the lack of a comprehensive system and organisation of national defence against cybernetic attacks on critical information infrastructure. The lack of adequate specialised units within central and local government institutions employing professionally prepared civil servants and experts responsible for cyber protection and security posed a significant challenge. The major reasons for the shortage of qualified personnel competent in cybersecurity matters in public institutions primarily included poor employment and salary conditions compared to those offered by the private sector.[29]

[28] "Указ Президента України №447/2021 Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року…". See also: "Щодо актуалізації використання кіберпростору як інструменту геополітичного суперництва. Аналітична записка", *NISS*, 28.09.2016, [online:] https://niss.gov.ua/doslidzhennya/informaciyni-strategii/schodo-aktualizacii-vikoristannya-kiberprostoru-yak (27.09.2022).

[29] "Указ Президента України №447/2021 Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року…".

Information and the cybernetic dimension of the war

The Russian attack on Ukraine on 24 February 2022 led to a complete shift in the geopolitical situation – it changed international relations not only in Central and Eastern Europe, but in the wider global dimension. The information dimension was an important part of the aggression that began on that date and included cyberattacks which formed an integral part of the war. It bears stressing that starting from 24 February 2022, we have entered a new stage of information war and measures aimed at counteracting it in two aspects: narrative, propaganda and disinformation, as well as the cybersecurity aspect.

As already noted, one of the key challenges in information security (taking cyber threats into account) is ensuring the continued operation and coordination of individual state administration bodies. The operation of these structures gained particular importance and value after 24 February 2022. It completely changed the institutional dimension of information policy as most central and local government bodies became involved in the policy after hostilities broke out. However, it is worth stressing that actions aimed at improving the coordination of activity in this regard and creating a comprehensive system focused on improving the state's information security had already begun at an earlier date. The system was composed of state institutions and bodies, specialised agendas and public benefit institutions that collaborated with the public sectors.[30]

The Ukrainian *State Communication and Information Protection Service* was one of the more important structures in this system. The institution was created on 23 February 2006 and acted as a special authority (at the executive level) within the information security system that was tasked with coordinating activities, counteracting and neutralising threats and cyberattacks.[31] The structure also includes the specialised CERT-UA team, whose most important tasks include combating computer threats, gathering data for analysis and keeping a national register of cyber-incidents.[32] In con-

[30] Cf.: "Актуальні питання розвитку державно-приватної взаємодії у сфері забезпечення кібербезпеки в Україні. Аналітична записка", *NISS*, 19.12.2017, [on-line:] https://niss.gov.ua/doslidzhennya/informaciyni-strategii/aktualni-pitannya-rozvitku-derzhavno-privatnoi-vzaemodii-u (27.09.2022).

[31] "Закон України Про Державну службу спеціального зв'язку та захисту інформації України", *Відомості Верховної Ради України*, no. 30, ст. 258 (2006), [on-line:] https://zakon.rada.gov.ua/laws/show/3475-15#Text (27.09.2022); "Державна служба спеціального зв'язку та захисту інформації України", *State Service for Special Communications and Information Protection of Ukraine*, [on-line:] https://cip.gov.ua/ua/statics/pro-derszhpeczv-yazku (27.09.2022).

[32] *Про CERT-UA* [on-line:] https://cert.gov.ua/about-us (27.09.2022).

nection with the Russian aggression, on 28 July 2022, President Zelenskyy signed an act that amended several key documents concerning information security and cyber threats. The act also created a new structure – the *Centre for Active Counteraction of Aggression in Cyberspace*. Its task was the central coordination of efforts in cybersecurity and the prevention of ongoing acts of sabotage and attacks in this sphere.[33]

It is worth noting that under the *Act on the Basic Principles of Protection of Ukraine's Cybersecurity*, adopted on 5 October 2017, the *Ukrainian National Security and Defence Council* ensures the coordination of practical security tasks. A special structure, the *State Cybersecurity Coordination Centre*, operates as part of the council. It was created on 27 January 2016 and is responsible for coordinating the operations and functioning of entities tasked with ensuring the protection and security of the Ukrainian state in this sphere.[34] The main tasks of the centre include policy coordination, analysing the operation of entities and authorities active in the area of cybersecurity, predicting and counteracting cyber threats, preparing legislation proposals and practical solutions that improve security. The centre is also responsible for actions in the area of interoperability and uniformisation of Ukrainian solutions with NATO standards in the sphere of cybersecurity.[35]

Another important structure in the system is the *Strategic Communications Centre*, which forms part of the *Ministry of Culture and Information Policy*. Its major tasks include preventing propaganda and disinformation and counteracting the negative image of Ukraine in the international arena created by Russia. The centre's activities primarily focus on developing and strengthening strategic communication, counteraction and the promotion of the Ukrainian narrative in the international arena, which is aimed at expanding and deepening collaboration with foreign partners. Collaboration and coordination of actions – and exchange of experiences and information with countries who deal with similar threats and have similar involvements in the area of information

[33] "Закон України Про внесення змін до деяких законів України щодо забезпечення формування та реалізації державної політики у сфері активної протидії агресії у кіберпросторі", *Verkhovna Rada of Ukraine*, [on-line:] https://zakon.rada.gov.ua/laws/show/2470-20#n10 (27.09.2022); "В Україні може з'явитися центр протидії агресії РФ у кіберпросторі — законопроект", *Sud.ua*, 4.07.2022 [on-line:] https://www.sud.ua/ru/news/publication/242993-v-ukrayini-mozhe-zyavitisya-tsentr-protidiyi-agresiyi-rf-u-kiberprostori-zakonoproekt (27.09.2022).

[34] "Закон України Про основні засади забезпечення кібербезпеки України", *Відомості Верховної Ради*, no. 45, ст. 403 (2017), [on-line:] https://zakon.rada.gov.ua/laws/show/2163-19#Text (27.09.2022).

[35] "Указ Президента України №242/2016 Про Національний координаційний центр кібербезпеки", *President of Ukraine: Official website*, [on-line:] https://www.president.gov.ua/documents/2422016-20141 (27.09.2022).

security – also form an important part of this aspect.[36] A vital role, in this regard, is also played by individual structures that form part of the *Security Service of Ukraine*, which is active in the area of information security – in particular, when it comes to counteracting propaganda and disinformation, as well as intercepting cyberattacks and defending against them.

Collaboration within these structures, including coordinating the functioning of media and its messaging, is one of the key aspects of strategic communication during the ongoing war. Russia engaged in active operations in this regard and is pushing the narrative that the aggression is a "special operation" that was necessary due to several reasons (e.g., to fight Ukrainian fascists and nationalists who discriminate against the Russian-speaking population and illegally took power in Ukraine).

Regarding Ukraine's information policy and strategic communication, it needs to be stressed that from the first days of the war, the Ukrainian authorities have engaged in cohesive actions and been presented a consistent narrative.

It is directed at its citizens, the international community and, at the beginning of the aggression, at Russians and Belarussians to encourage the citizens of these countries to actively oppose and protest against the attack on Ukraine. Announcements and appeals to stay calm, assurances that the Ukrainian army is ready to repulse the attack and defend its country, and calls to adopt patriotic attitudes and engage in civil resistance were extremely important from the perspective of effectiveness and defence of the country. In the international dimension, the main narrative is focused on counteracting Russian propaganda by spotlighting Russia's aggression on a sovereign and independent country, constituting a total violation of international standards and laws and the world order created after World War II. Ukraine also stresses that the attack was completely unfounded and actively informs the international community about the atrocities of war, attacks on civil infrastructure and defenceless people – and genocide taking place in areas occupied by Russian forces – by calling on the international community to impose sanctions and limit its cooperation with the aggressor. It needs to be stressed that President Volodymyr Zelenskyy has become a key figure when it comes to strategic communication. His decision to remain in Kyiv in the first days of the war was an important aspect that helped keep the morale of Ukrainian soldiers up and foil Russia's plans of a quick conquest of Ukraine.[37]

[36] "Центр стратегічних комунікацій", *Centre for Strategic Communication*, [on-line:] https://spravdi.gov.ua/pro-nas (27.09.2022).

[37] A.M. Dyner, M. Piechowska, "Ukraine's Wartime Information Strategy", *Bulletin PISM*, 4.04.2022. See also: "Бій за Африку: як українська дипломатія розширює горизонти та бореться з впливом росії на континенті", *Democratic Initiatives*, 1.11.2022, [on-line:] https://dif.org.ua/article/

As regards the cybernetic dimension of the ongoing war, of particular note is that cyberattacks against Ukraine intensified in the months leading up to the aggression. The attacks were primarily aimed at strategic state management sectors and critical infrastructure systems. On the eve of the Russian aggression, one of the largest cyberattacks in Ukraine's history took place. A mass DDoS (distributed denial-of-service) attack was launched against websites of the Ukrainian government and the online system of one of Ukraine's largest banks. Another cyberattack took place on the eve of the attack and was again aimed against government websites, critical infrastructure and the *Viasat* satellite network. The attacks continued in subsequent weeks and were most frequent in the first three months of the aggression. Due to these risks, the Ukrainian authorities decided to transfer their data to servers abroad and enlisted the services of global commercial companies for this purpose. In subsequent weeks of the war, several dozen central government bodies decided to follow suit and transfer databases of key importance abroad from the perspective of national security.[38]

As previously noted, an important task is coordinating actions by several bodies responsible for cybersecurity, including specialised structures of the *Security Service of Ukraine* – which is responsible for counteracting disinformation and propaganda, as well as coordinating defence against cyberattacks.[39] It should be noted that these are unseen actions that take place in the computer world, but they constitute an integral part of the ongoing war. Ukrainian experts react to threats in this sphere on an ongoing basis. According to the *Department of Cybersecurity of the Security Service of Ukraine*, between the start of the aggression and November 2022, Russia launched over 3,500 cyberattacks against Ukraine, with over ten attacks occurring daily.[40]

biy-za-afriku-yak-ukrainska-diplomatiya-rozshiryue-gorizonti-ta-boretsya-z-vplivom-rosii-na-kontinenti?fbclid=IwAR1pqtJpEnhJKlaC-INxYGQzDchhy98vVBJ-7UnvtHv_E4OQY4OgOW88OFQ (27.09.2022).

[38] Д. Петровський, "Перша світова кібервійна", *Unian*, 3.10.2022, [on-line:] https://www.unian.ua/techno/persha-svitova-kiberviyna-yak-ukrajina-boretsya-na-drugomu-fronti-11998566.html (28.09.2022); "Кібератака в Україні 15 лютого була найбільшою в історії держави: в Кабміні назвали вартість", *Unian*, 16.02.2022, [on-line:] https://www.unian.ua/techno/communications/kiberataka-v-ukrajini-15-lyutogo-bula-naybilshoyu-v-istoriji-derzhavi-v-kabmini-nazvali-vartist-11706571.html (28.09.2022).

[39] "СБУ ліквідувала у Дніпрі ворожу ботоферму, яка створила майже 10 тис. фейкових акаунтів для «розгону» кремлівської пропаганди в ЄС", *Security Service of Ukraine*, 20.10.2022, [on-line:] https://ssu.gov.ua/novyny/sbu-likviduvala-u-dnipri-vorozhu-botofermu-yaka-stvoryla-maizhe-10-tys-feikovykh-akauntiv-dlia-rozghonu-kremlivskoi-propahandy-v-yes (28.09.2022).

[40] "рф щодня здійснює понад 10 кібератак на стратегічні об'єкти України, – керівник Департаменту кібербезпеки СБУ", *Security Service of Ukraine*, 9.11.2022, [on-line:] https://ssu.gov.ua/novyny/rf-shchodnia-zdiisniuie-ponad-10-kiberatak-na-stratehichni-obiekty-ukrainy-kerivnyk-departamentu-kiberbezpeky-sbu (28.09.2022).

As previously noted, the activities of central government authorities in the area of information security were complemented by actions taken by structures on the regional level and close cooperation with public benefit institutions and individual specialists. These entities demonstrated significant flexibility in action and efficiency in combating information and cybernetic threats in information security. Cooperation, in this regard, intensified following Russia's aggression, and the mutual exchange of experiences between the non-governmental sector and state structures impacted the effectiveness of crisis management in the area of information security.

It needs to be stressed that many governmental and grassroots initiatives aimed at preventing hacking attacks appeared in connection with the outbreak of the war. One of the more effective initiatives was the creation of an 'IT army' by the *Ministry of Digitisation of Ukraine* – the product of combined forces and efforts of companies representing various strategic sectors of the state, IT experts and volunteers interested in supporting this type of activities who received adequate training. According to available information, the IT army may number up to 200,000 specialists actively participating in cyber war. One of their more effective and widely publicised achievements was their hacking of *Wagner Group*'s servers and identification of those of its members who participated in the aggression on Ukraine. Reports in the media also indicate that in late August and early September 2022, the group attacked and disabled over 2,400 Russian portals and websites (including such powerful ones as *Gazprombank*, *KreditBank Moscow*, *Sovcombank*, *Rambler*, *Gazeta.ru. MK*).[41] It, therefore, needs to be stressed that Ukrainians do not limit themselves exclusively to defence, but also engage in active counteraction by forcing the attackers to defend and limit their offensive action. This translates into a reduced number of attacks during this time, which points to the effectiveness of the action taken by Ukrainians.[42]

[41] Д. Петровський, *op. cit.*

[42] В. Орлова, "Как работает IT-армия Украины и какие победы уже на ее счету. Объяснение Федорова", *RBC*, 27.04.2022, [on-line:] https://www.rbc.ua/rus/news/rabotaet-it-armiya-ukrainy-kakie-pobedy-schetu-1651046717.html; "IT-армія України: чим вона займається та які перемоги вже на її рахунку", *Unian*, 27.04.2022, [on-line:] https://www.unian.ua/techno/communications/it-armiya-ukrajini-chim-vona-zaymayetsya-ta-yaki-peremogi-vzhe-na-jiji-rahunku-11803026.html (28.09.2022); "Україна веде активний контрнаступ на кіберфронті – Ілля Вітюк", *Security Service of Ukraine*, 17.10.2022, [on-line:] https://ssu.gov.ua/novyny/ukraina-vede-aktyvnyi-kontrnastup-na-kiberfronti-illia-vitiuk (28.09.2022).

Summary

Based on the research process and verification of the formulated research hypothesis we can conclude that Ukraine has significantly increased its effectiveness and capabilities in terms of information resilience and efficiency of security policy. The process was impacted by the implementation of comprehensive decisions and actions in respect of individual aspects of information security, such as legislative and legal actions and improvement of information infrastructure. The annexation of Crimea in 2014 and the subsequent conflict in the eastern oblasts of Ukraine constituted a breakthrough in the formation of Ukraine's information security policy. The events marked a turning point at which Ukraine was forced to react to the propaganda and disinformation activities that Russia engaged in on a mass scale, both internally in respect of Ukrainian citizens, and in respect of the wider international community. It was at this stage that Ukrainian authorities made further key decisions aimed at improving their information security and counteracting the increasing threat posed by Russia in this area. This was reflected in the successive adoption of security strategies and specialised documents focusing directly on information security and cybersecurity. Ukraine followed the implementation of legal regulations with practical actions aimed at improving its information security and counteracting threats in this area. After Russia began its aggression in early 2022, Ukraine was therefore able to build on its experiences of the past few years and showed good effectiveness in this area. Ukraine has been able to effectively counteract and combat propaganda and disinformation, and has been taking actions in the area of strategic communication in order to strengthen its own narrative on the Russian aggression and the ongoing war on the international arena. Confrontation in the cyberspace is an integral part of the conflict and Ukraine has been waging war effectively in this area as well, largely based on its experiences of the past few years.

In summary, we can conclude that the information security pursued by Ukraine in recent years, despite its many flaws and issues, has allowed the country to gain experience and prepare for defence, which has been extremely important and efficiently utilised in the course of the current aggression. The ongoing war has again confirmed that in the context of both strategic communication and cybersecurity, aspects related to information have an extremely important role to play in the modern society, both in terms of resilience of states and tools used for waging war. Further analysis of the ongoing war in terms of its information aspect are therefore required and this area of national security and defence must continue to be improved, taking into account

Ukraine’s experiences and conclusions in terms of the ongoing fight in the area of strategic communication and cybersecurity.

References

“7 strategìčnih cìlej ìnformacìjnoï bezpeki Ukraïni” [“7 стратегічних цілей інформаційної безпеки України”], *LexInform*, [on-line:] https://lexinform.com.ua/zakonodavstvo/7-strategichnyh-tsilej-informatsijnoyi-bezpeky-ukrayiny/.

“Aktual’nì pitannâ rozvitku deržavno-privatnoï vzaêmodìï u sferì zabezpečennâ kìberbezpeki v Ukraïnì. Analìtična zapiska” [“Актуальні питання розвитку державно-приватної взаємодії у сфері забезпечення кібербезпеки в Україні. Аналітична записка”], *NISS*, 19.12.2017, [on-line:] https://niss.gov.ua/doslidzhennya/informaciyni-strategii/aktualni-pitannya-rozvitku-derzhavno-privatnoi-vzaemodii-u.

“Analìz Strategìï ìnformacìjnoï bezpeki v porìvnânnì z činnoû Doktrinoû ìnformacìjnoï bezpeki” [“Аналіз Стратегії інформаційної безпеки в порівнянні з чинною Доктриною інформаційної безпеки”], *Institute of Mass Information*, 29.04.2021, [on-line:] https://imi.org.ua/monitorings/analiz-strategiyi-informatsijnoyi-bezpeky-v-porivnyanni-z-chynnoyu-doktrynoyu-informatsijnoyi-i38852.

“Bìj za Afriku: âk ukraïns’ka diplomatìâ rozšìrûê gorizonti ta boret’sâ z vplivom rosìï na kontinentì” [“Бій за Африку: як українська дипломатія розширює горизонти та бореться з впливом росії на континенті”], *Democratic Initiatives*, 1.11.2022, [on-line:] https://dif.org.ua/article/biy-za-afriku-yak-ukrainska-diplomatiya-rozshiryue-gorizonti-ta-boretsya-z-vplivom-rosii-na-kontinenti?fbclid=IwAR1pqtJpEnhJKlaC-INxYGQzDchhy98vVBJ-7UnvtHv_E4OQY4OgOW88OFQ.

“Centr strategìčnih komunìkacìj” [“Центр стратегічних комунікацій”], *Centre for Strategic Communication*, [on-line:] https://spravdi.gov.ua/pro-nas.

“Deržavna služba specìal’nogo zv’âzku ta zahistu ìnformacìï Ukraïni” [“Державна служба спеціального зв’язку та захисту інформації України”], *State Service for Special Communications and Information Protection of Ukraine*, 1.06.2022, [on-line:] https://cip.gov.ua/ua/statics/pro-derszhpeczv-yazku.

“Doktrina ìnformacìjnoï bezpeki Ukraïni – ce liše deklaracìâ – eksperti” [“Доктрина інформаційної безпеки України – це лише декларація – експерти”], *Radio Svoboda*, 27.02.2017, [on-line:] https://www.radiosvoboda.org/a/28336852.html.

Dovhan O.D., Tkačuk T.Û., “Sistema ìnformacìjnoï bezpeki Ukraïni: ontologìčnì vimìri”, *Ìnformacìâ ì pravo* [Довгань О.Д., Ткачук Т.Ю., “Система інформаційної безпеки України: онтологічні виміри”, *Інформація і право*, vol. 1, no. 24 (2018), pp. 90–97.

Dubov D., “Formuûči novu Strategìû kìberbezpeki Ukraïni: či zmožemo uniknuti pomilok peršoï sprobi strateguvannâ?” [Дубов Д., “Формуючи нову Стратегію кібербезпеки України: чи зможемо уникнути помилок першої спроби стратегування?”], *NISS*, 27.01.2021, [on-line:] https://niss.gov.ua/doslidzhennya/informaciyna-politika/formuyuchi-novu-strategiyu-kiberbezpeki-ukraini-chi-zmozhemo.

Dyner A.M., Piechowska M., “Ukraine’s Wartime Information Strategy”, *Bulletin PISM*, 4.04.2022, https://doi.org/10.1177/009286157000400119.

Isakova T.O., “Propaganda sprâmovana na rozpalûvannâ nacìonal’noï ta mìžnacìonal’noï vorožnečì: problemi viznačennâ ta protidìï”, *Analìtična zapiska*, no. 2, Serìâ «Ìnformacìjnì strategìï» [Ісакова Т.О., “Пропаганда спрямована на розпалювання національної та міжнаціональної ворожнечі: проблеми визначення та протидії”, *Аналітична записка*, no. 2, Серія «Інформаційні стратегії»], *NISS*, 2.03.2015, [on-line:] https://niss.gov.ua/doslidzhennya/informaciyni-strategii/propaganda-spryamovana-na-rozpalyuvannya-nacionalnoi-ta.

“IT-armìâ Ukraïni: čim vona zajmaêt’sâ ta âkì peremogi vže na ïï rahunku” [“IT-армія України: чим вона займається та які перемоги вже на її рахунку”], *Unian*, 27.04.2022, [on-line:] https://www.unian.ua/techno/communications/it-armiya-ukrajini-chim-vona-zaymayetsya-ta-yaki-peremogi-vzhe-na-jiji-rahunku-11803026.html.

Jaitner M.L., “Russian Information Warfare: Lessons from Ukraine”, in K. Geers (ed.), *Cyber War in Perspective: Russian Aggression against Ukraine*, NATO CCD COE Publications, Tallinn 2015.

“Kìberataka v Ukraïnì 15 lûtogo bula najbìl’šoû v ìstorìï deržavi: v Kabmìnì nazvali vartìst’” [“Кібератака в Україні 15 лютого була найбільшою в історії держави: в Кабміні назвали вартість”], *Unian*, 16.02.2022, [on-line:] https://www.unian.ua/techno/communications/kiberataka-v-ukrajini-15-lyutogo-bula-naybilshoyu-v-istoriji-derzhavi-v-kabmini-nazvali-vartist-11706571.html.

“Mìžnarodnij dosvìd vprovadžennâ medìagramotnostì dlâ okremih cìl’ovih grup: možlivostì dlâ Ukraïni” [“Міжнародний досвід впровадження медіаграмотності для окремих цільових груп: можливості для України”], *NISS*, 14.05.2019, [on-line:] https://niss.gov.ua/doslidzhennya/informaciyni-strategii/mizhnarodniy-dosvid-vprovadzhennya-mediagramotnosti-dlya.

“Nova Strategìâ kìberbezpeki Ukraïni” [„Нова Стратегія кібербезпеки України”], *LexInform*, [on-line:] https://lexinform.com.ua/zakonodavstvo/nova-strategiya-kiberbezpeky-ukrayiny/.

Novytskyi V., “Strategìčnì zasadi zabezpečennâ ìnformacìjnoï bezpeki v sučasnih umovah”, *Ìnformacìâ ì pravo* [Новицький В., “Стратегічні засади забезпечення інформаційної безпеки в сучасних умовах”, *Інформація і право*], vol. 1, no. 40 (2022), pp. 114–115.

Orlova V., “Kak rabotaet IT-armiâ Ukrainы i kakie pobedы uže na ee sčetu. Obъâsnenie Fedorova” [Орлова В., “Как работает IT-армия Украины и какие победы уже на ее счету. Объяснение Федорова”], *RBC*, 27.04.2022, [on-line:] https://www.rbc.ua/rus/news/rabotaet-it-armiya-ukrainy-kakie-pobedy-schetu-1651046717.html.

Petrovsky D., “Perša svìtova kìbervìjna” [Петровський Д., “Перша світова кібервійна”], *Unian*, 3.10.2022, [on-line:] https://www.unian.ua/techno/persha-svitova-kiberviyna-yak-ukrajina-boretsya-na-drugomu-fronti-11998566.html.

Popova T., “Ŝo označaê «Doktrina ìnformacìjnoï bezpeki Ukraïni»?” [Попова Т., “Що означає «Доктрина інформаційної безпеки України»?”], *Radio Svoboda*, 28.02.2017, [on-line:] https://www.radiosvoboda.org/a/28337376.html.

“Prezident uvìv u dìû rìšennâ RNBO pro Strategìû ìnformacìjnoï bezpeki” [“Президент увів у дію рішення РНБО про Стратегію інформаційної безпеки”], *Ukrinform*, 28.12.2021, [on-line:] https://www.ukrinform.ua/rubric-polytics/3376906-prezident-uviv-u-diu-risenna-rnbo-pro-strategiu-informacijnoi-bezpeki.html.

“Prezident zatverdiv Strategìû ìnformacìjnoï bezpeki: ŝo peredbačeno” [“Президент затвердив Стратегію інформаційної безпеки: що передбачено”], *Jurliga*, 29.12.2021, [on-line:] https://jurliga.ligazakon.net/news/208447_prezident-zatverdiv-strategyu-nformatsyno-bezpeki-shcho-peredbacheno.

“rf ŝodnâ zdìjsnûê ponad 10 kìberatak na strategìčnì ob'̀ekti Ukraïni, – kerìvnik Departamentu kìberbezpeki SBU” [“рф щодня здійснює понад 10 кібератак на стратегічні об’єкти України, – керівник Департаменту кібербезпеки СБУ”], *Security Service of Ukraine*, 9.11.2022, [on-line:] https://ssu.gov.ua/novyny/rf-shchodnia-zdiisniuie-ponad-10-kiberatak-na-stratehichni-obiekty-ukrainy-kerivnyk-departamentu-kiberbezpeky-sbu.

“SBU lìkvìduvala u Dnìprì vorožu botofermu, âka stvorila majže 10 tis. fejkovih akauntìv dlâ «rozgonu» kremlìvs’koï propagandi v ÊS” [“СБУ ліквідувала у Дніпрі ворожу ботоферму, яка створила майже 10 тис. фейкових акаунтів для «розгону» кремлівської пропаганди в ЄС”], *Security Service of Ukraine*, 20.10.2022, [on-line:] https://ssu.gov.ua/novyny/sbu-likviduvala-u-dnipri-vorozhu-botofermu-yaka-stvoryla-maizhe-10-tys-feikovykh-akauntiv-dlia-rozghonu-kremlivskoi-propahandy-v-yes.

“Ŝodo aktualìzacìï vikoristannâ kìberprostoru âk ìnstrumentu geopolìtičnogo supernictva. Analìtična zapiska” [“Щодо актуалізації використання кіберпростору як інструменту геополітичного суперництва. Аналітична записка”], *NISS*, 28.09.2016, [on-line:] https://niss.gov.ua/doslidzhennya/informaciyni-strategii/schodo-aktualizacii-vikoristannya-kiberprostoru-yak.

“Strategìû ìnformacìjnoï bezpeki-2025 prijnâto: ŝo zmìnit’sâ u sferì cifrovih prav?” [“Стратегію інформаційної безпеки-2025 прийнято: що зміниться у сфері цифрових прав?”], *Digital Security Lab*, 18.01.2022, [on-line:] https://dslua.org/publications/stratehiiu-informatsiynoi-bezpeky-2025-pryyniato-shcho-zminytsia-u-sferi-tsyfrovykh-prav/.

“Ukaz Prezidenta Ukraïni №242/2016 Pro Nacìonal’nij koordinacìjnij centr kìberbezpeki” [“Указ Президента України №242/2016 Про Національний координаційний центр кібербезпеки”], *President of Ukraine: Official website*, [on-line:] https://www.president.gov.ua/documents/2422016-20141.

“Ukaz Prezidenta Ukraïni №447/2021 Pro rìšennâ Radi nacìonal’noï bezpeki ì oboroni Ukraïni vìd 14 travnâ 2021 roku «Pro Strategìû kìberbezpeki Ukraïni»” [“Указ Президента України №447/2021 Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»”], *President of Ukraine: Official website*, [on-line:] https://www.president.gov.ua/documents/4472021-40013.

“Ukaz Prezidenta Ukraïni №47/2017 Pro rìšennâ Radi nacìonal’noï bezpeki ì oboroni Ukraïni vìd 29 grudnâ 2016 roku «Pro Doktrinu ìnformacìjnoï bezpeki Ukraïni»” “Указ Президента України №47/2017 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»”, *President of Ukraine: Official website*, [on-line:] https://www.president.gov.ua/documents/472017-21374.

“Ukaz Prezidenta Ukraïni №685/2021 Pro rìšennâ Radi nacìonal’noï bezpeki ì oboroni Ukraïni vìd 15 žovtnâ 2021 roku «Pro Strategìû ìnformacìjnoï bezpeki»” [“Указ Президента України №685/2021 Про рішення Ради національної безпеки і оборони України від

15 жовтня 2021 року «Про Стратегію інформаційної безпеки»"], *President of Ukraine: Official website*, [on-line:] https://www.president.gov.ua/documents/6852021-41069.

"Ukaz Prezidenta Ukraïni №96/2016 Pro rìšennâ Radi nacìonal'noï bezpeki ì oboroni Ukraïni vìd 27 sìčnâ 2016 roku «Pro Strategìû kìberbezpeki Ukraïni»" ["Указ Президента України №96/2016 Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»"], *President of Ukraine: Official website*, [on-line:] https://www.president.gov.ua/documents/962016-19836.

"Ukaz Prezidenta Ukraïni Pro rìšennâ Radi nacìonal'noï bezpeki ì oboroni Ukraïni vìd 14 veresnâ 2020 roku 'Pro Strategìû nacìonal'noï bezpeki Ukraïni'" ["Указ Президента України Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року 'Про Стратегію національної безпеки України'"], *Verkhovna Rada of Ukraine*, [on-line:] https://zakon.rada.gov.ua/laws/show/392/2020#Text.

"Ukaz Prezidenta Ukraïni Pro rìšennâ Radi nacìonal'noï bezpeki ì oboroni Ukraïni vìd 14 veresnâ 2020 roku 'Pro Strategìû nacìonal'noï bezpeki Ukraïni'" ["Указ Президента України Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року 'Про Стратегію національної безпеки України'"], *Verkhovna Rada of Ukraine*, [on-line:] https://zakon.rada.gov.ua/laws/show/392/2020#Text.

"Ukraïna vede aktivnij kontrnastup na kìberfrontì – Ìllâ Vìtûk" ["Україна веде активний контрнаступ на кіберфронті – Ілля Вітюк"], *Security Service of Ukraine*, 17.10.2022, [on-line:] https://ssu.gov.ua/novyny/ukraina-vede-aktyvnyi-kontrnastup-na-kiberfronti-illia-vitiuk.

"V Ukraïnì može z'âvitisâ centr protidìï agresìï RF u kìberprostorì – zakonoproekt" ["В Україні може з'явитися центр протидії агресії РФ у кіберпросторі – законопроект"], *Sud.ua*, 4.07.2022, [on-line:] https://www.sud.ua/ru/news/publication/242993-v-ukrayini-mozhe-zyavitisya-tsentr-protidiyi-agresiyi-rf-u-kiberprostori-zakonoproekt.

"Zakon Ukraïni Pro Deržavnu službu specìal'nogo zv'âzku ta zahistu ìnformacìï Ukraïni", *Vìdomostì Verhovnoï Radi Ukraïni* ["Закон України Про Державну службу спеціального зв'язку та захисту інформації України", *Відомості Верховної Ради України*], no. 30, ст. 258 (2006), [on-line:] https://zakon.rada.gov.ua/laws/show/3475-15#Text.

"Zakon Ukraïni Pro osnovnì zasadi zabezpečennâ kìberbezpeki Ukraïni", *Vìdomostì Verhovnoï Radi* ["Закон України Про основні засади забезпечення кібербезпеки України"], *Відомості Верховної Ради*, no. 45, ст. 403 (2017), [on-line:] https://zakon.rada.gov.ua/laws/show/2163-19#Text.

"Zelens'kij zatverdiv Strategìû ìnformacìjnoï bezpeki Ukraïni" ["Зеленський затвердив Стратегію інформаційної безпеки України"], *Institute of Mass Information*, 29.12.2021, [on-line:] https://imi.org.ua/news/zelenskyj-zatverdyv-strategiyu-informatsijnoyi-bezpeky-ukrayiny-i43121.

Zhovtenko T., "Gìbridna vìjna: anatomìâ ìnstrumentarìû j peremogi" ["Гібридна війна: анатомія інструментарію й перемоги"], *Democratic Initiatives*, 3.11.2022, [on-line:] https://dif.org.ua/article/gibridna-viyna-anatomiya-instrumentariyu-y-peremogi.

"Žurnalìstika na teritorìï Ukraïni v umovah gìbridnoï vìjni: mežì ta možlivostì deržavnogo regulûvannâ. Analìtična zapiska" ["Закон України Про внесення змін до деяких законів України щодо забезпечення формування та реалізації державної політики у сфері активної протидії агресії у кіберпросторі”], *Verkhovna Rada of Ukraine*, 28.07.2022, [on-line:] https://zakon.rada.gov.ua/laws/show/2470-20#n10.

“Журналістика на території України в умовах гібридної війни: межі та можливості державного регулювання. Аналітична записка”, *NISS*, [on-line:] https://niss.gov.ua/doslidzhennya/informaciyni-strategii/zhurnalistika-na-teritorii-ukraini-v-umovakh-gibridnoi-viyni.

Information security is one the key aspects of modern security and its importance has been significantly increasing in contemporary international relations. This publication presents the results of studies on several key aspects related to this issue. The publication contains results of research on considerations related to information security and its implementation, as well as research on social media, analysed through the lens of the object and subject of disinformation activities.

WYDAWNICTWO
KSIĘGARNIA AKADEMICKA
Sp. z o.o. Kraków

https://akademicka.pl

ISBN 978-83-8138-826-9
9 788381 388269