ISSN 2415-8496 – Print
ISSN 3083-6794 – Online
Obraz, 2025. Vol.3 (49).

UDC: 007 : 304 : 659.3
https://doi.org/10.21272/Obraz.2025.3(49)-6-17

WAR IN UKRAINE: EDUCATING JOURNALISTS FOR CRISIS REPORTING

KOWALIK Krzysztof[1], PhD with habilitation,
ORCID – https://orcid.org/0000-0001-8511-6851;
LIASHENKO Iryna[2], PhD (Pedagogy), Associate Professor,
ORCID – https://orcid.org/0000-0003-4211-5116;
BONDARENKO Olena[2,3], PhD (Philology), Associate Professor,
ORCID – https://orcid.org/0000-0002-2369-774X.

[1] University of Warsaw, Poland,
[2] Sumy State University, Ukraine.
[3] Corresponding author Bondarenko O., e-mail: ol.bondarenko@journ.sumdu.edu.ua

Article received by the editorial office on 10/08/2025
Submitted after editing on 10/09/2025
Recommended for publication on 06/11/2025

Citation: *Kowalik, K., Liashenko I. & Bondarenko, O. (2025). War in Ukraine: Educating Journalists for Crisis Reporting. Obraz, 3 (49), 6–17. https://doi.org/10.21272/Obraz.2025.3(49)-6-17.*

The Introduction. The article analyzes the challenges and new competencies required of journalists reporting on the war in Ukraine warsince 2022, with particular emphasis on the role of digital technologies, OSINT (open-source intelligence) tools, and generative artificial intelligence.

Relevance of the study. In the context of full-scale war, Ukrainian media faced the necessity not only of providing reliable information to the public and countering disinformation, but also of rapidly adapting to new threats such as propaganda, fake news, and deepfakes.

Methodology. The study is based on case analyses of Ukrainian journalists' activities, the use of digital verification tools, and a review of scientific literature and media materials from 2022–2025. Advanced search techniques and analytical tools such as PinPoint and Notebook LM were employed to identify a catalogue of the most important tools and competencies essential for journalistic work in wartime conditions.

Results. The findings indicate that key skills include the use of open sources, data analysis, fact-checking, and proficiency with AI tools, all while adhering to principles of ethics and information security.

Conclusions. The experiences of Ukrainian media highlight the necessity of continuous journalist education in new technologies and the development of resilience to informational and psychological pressure from adversaries. The article formulates recommendations for journalism education, emphasizing the need to develop a catalogue of digital tools and competencies that will enable the media to maintain standards of reliability and credibility in times of crisis.

Keywords: *media, journalism, Ukraine, war, education, crises, OSINT, AI, technologies.*

Introduction. The Russian attack on Ukraine in 2022 and the ensuing military operations conducted during a full-scale war have sparked a renewed discussion regarding the role of the media in times of crisis and in circumstances that provoke both domestic and international societal shock. Reporting directly from the front lines, as well as covering the situation within the country, required journalists – and other media professionals – to develop and employ specific skills. Some of them already had experience from previous Russian aggressions in 2014 (the annexation of Crimea and parts of the Donetsk and Lugansk regions; see more on Ukrainian journalists' experiences) [4], [5]. However, the scale of the war after 2022 demanded new competencies, primarily digital ones, from a much larger number of media workers engaged in reporting on the atrocities committed by the enemy. Additionally, Russia's hybrid actions and sophisticated propaganda posed – and continue to pose – a threat to the public mood of Ukrainians and the construction of an accurate portrayal of the conflict. From the outset of Russian aggression, Ukrainian media had to counteract disinformation and hostile narratives. It became essential to present the wartime reality based on reliable, verified information. This is not an easy task, as reporters must maintain objectivity while avoiding becoming valuable sources of information for enemy forces, which could increase the aggressor's potential.

Technological transformations of the 21st century have significantly changed both journalistic practice and media education in general. Two key tools that are increasingly being integrated into this area are OSINT (Open Source Intelligence) and artificial intelligence (AI). In the context of the Russian-Ukrainian war, the spread of disinformation and cyber threats make both tools critical for the formation of a new digital literacy for journalists and media consumers. The first examples of the use of OSINT in Ukraine date back to 2004–2010, when investigative journalists began to actively open registries, databases, domain analytics, etc. A turning point in the systemic deployment of OSINT occurred after Euromaidan and the onset of the war in Donbas in 2014, with the emergence of public initiatives such as InformNapalm, Euromaidan Press, and Bellingcat, which mobilized Ukrainian volunteers in analyzing open-source data to investigate crimes committed by Russian forces.

The work of a journalist during the era of fake news and deepfakes [20], as well as during crises or large-scale conflicts, requires both competence and responsibility. The importance of credible information during mass threats was demonstrated by the COVID-19 pandemic [18]. On the one hand, during armed conflict, journalists must perform their duties reliably; on the second hand, they are subject to the constraints of self-censorship or military censorship. Wartime circumstances require not only the ability to select information and the language of communication (the graphic nature of images or videos, emotions conveyed in reports, etc.) but also a change in working conditions regarding methods of information verification. In peacetime, a mistake might result in a correction or a legal process; in wartime, it can mean the death of innocent people or losses within the military ranks. The situation in Ukraine indicates that the contemporary battlefield reporter, a journalist engaged in such drastic times, must possess skills and competencies that enable the media to construct an objective picture of the situation during societal upheaval.

The aim of this article is to identify those elements of journalistic work in wartime conditions related to technology - especially within the framework of OSINT - open-source intelligence [14] and genAI - generative artificial intelligence [8] – which can support journalists in effectively verifying information and sources during exposure to fake news and deepfakes. The researches pose the following research question: What digital skills and competencies should a reporter or journalist working in crisis situations, particularly in the context of armed conflict, possess? The conclusions may indicate directions for educating both current journalists and future professionals, as well as for defining a catalogue of digital tools that will help the media maintain standards during crises, especially armed conflicts.

Research materials and methods. The study encompasses case analyses of Ukrainian media operations, the digital activities of journalists and reporters, and their methods of utilizing online tools to maintain accuracy and objectivity in reporting from February 2022 – the onset of Russia's attack on Ukraine – through April 2025. To construct a comprehensive source base, two methodological approaches were employed:

1. The search for high-quality media content concerning the application of OSINT and AI by journalists. Advanced Google search functions, including search operators , were used. Additionally, "deep search" was supported by large language models such as GPT , Gemini , and the Perplexity service , which aggregates several language models.

2. Advanced searches for articles and literature presenting cases of Ukrainian media work and platforms specializing in OSINT and AI. Recognized international scientific literature aggregators, such as Scopus and Web of Science , were utilized.

Keyword searches were conducted in both English and Ukrainian, requiring their co-occurrence to narrow results to sources directly relevant to the research topic. Keywords and phrases included: OSINT, open-source intelligence, digital verification tools, military disinformation, war fact-checking, Ukrainian media verification, information warfare, artificial intelligence. In scientific databases, terms such as fact checking Ukraine, Ukraine war, journalism fact checking, OSINT, and artificial intelligence were used.

The "snowball effect" [21] was applied: if a relevant online service with further links to additional sources was found, these were subsequently verified. For example, a search for sources tagged "information verification" might also yield materials with "digital verification tools", which in turn describe OSINT or AI techniques, leading to the use of OSINT and AI tags in the next step. Articles were filtered for authenticity and credibility, excluding those lacking clear sources or with unverifiable origins. The domain (especially Ukrainian .ua) and portal or publisher titles were decisive factors, particularly for foreign media; materials from Russian domains (.ru) were excluded.

Collected materials were downloaded as PDFs and analyzed using two applications: PinPoint, which enables automatic searching of large datasets (texts, spreadsheets, images, audio, and online materials), and Notebook LM , which supports data searching, contextual understanding, and correlation. Both services use language models provided by Alphabet (Google's parent company) and allow interaction with sources.

Subsequently, a catalogue of tools used by Ukrainian and foreign media for war-related information verification was compiled. Based on the characteristics and functionalities of these platforms and applications, an attempt was made to specify their uses and objectives for media professionals. The resulting list was compared with existing recommendations for journalism education published by international organizations.

Discussion. Information gathering techniques within OSINT first appeared during World War II, when the potential of open sources of information was recognized [10]. The term was coined in the literature in 1993 and focused on data collection methodologies, but did not exclude data analysis [10]. With the development of technology, especially the rapidly growing databases and online tools, OSINT has become a tool allowing the verification of an increasingly wide range of information related to media, business, health, and criminal matters. Human rights violations and the need to document them became a significant catalyst for change. There arose a necessity to create OSINT procedures and methodologies that would be recognized as proper and objective. In 2022, the United Nations Human Rights Office of The High Commissioner published the "Berkeley Protocol on Digital Open Source Investigations" [9]. This document specifies the procedures that must be met for evidence collected through OSINT to be accepted and recognized by institutions such as law enforcement agencies and courts. Controversial situations related to human rights violations have existed for years, but events such as increasing disinformation, the phenomena of fake news and deepfake, the pandemic, and armed conflicts have intensified the need to establish standards for examining publicly available sources. However, it is important to remember that OSINT also poses threats, which may arise from privacy violations or the exploration of data sources without any oversight [13].

In media and journalism, there has been increased pressure to verify information sources and filter out those contaminated by lies or propaganda. The catalyst for change was the Russian attack on Ukraine. Journalists play an important role during armed conflict or other mass crises, as they should be the main source of reliable information for society. They must attract attention, respond to the target audience, and adapt the format of the message to perceptual capabilities, which in turn requires the development of new competencies. This was especially recognized by Ukrainian journalists who already had wartime experience [5, pp. 219-222].

An important vector for future journalism education in times of war and upheaval is the experience of those directly involved in creating messages from the battlefield. The time of conflict involves work on the front line but also in local newsrooms. Ukrainian experiences indicate the need to focus on skills and competencies that seem essential for journalism in times of conflict and on the battlefield (both at the front and in the rear). Many of these aspects are presented in publications about the work of Ukrainian journalists. They identified several areas where education can significantly increase the effectiveness of journalism during war or other large-scale crises. One of the fundamental duties is to ensure the reliability of the message and access to credible information, especially during periods of intensified enemy propaganda. An example after February 24, 2022, is the rapid increase in interest in the Facebook profile of the Ukrainian Land Forces Command – from 80,000 to over 800,000 people – and the launch of a Telegram channel [5, pp. 121-132]. There was a growing need to direct audiences to sources not contaminated by enemy propaganda, such as official services like the government Ukrinform or services like Censor, Radio Svoboda [5, pp. 42-51]. Information warfare also involves actions related to the psychological pressure exerted by the enemy on victims, which takes place on many levels. Journalists' experience can also point to mistakes made by authorities who, unaware of their decisions, endanger their own armed forces. An example is presented in a publication of reporters' memoirs, which indicated informational neglect on publicly available online maps where the enemy could find unmasked Ukrainian military objects after 11 months of war [5, pp. 135-140]. Those experienced in creating wartime messages emphasize the technological aspect of a reporter's work, such as data journalism (allowing for data analysis and visualization, use of public open databases, numerous internet sources, etc.). The Ukrainian example clearly indicates that journalism operating within OSINT can be a weapon, allowing for maintaining high quality and credibility of materials. Tools such as scrapers (programs and applications that allow for real-time monitoring, collecting, and analyzing large streams of information) support the detection of potential problems and, importantly, help to understand their causes. Such actions "allow maintaining the combat capability of Ukrainian media" [5, pp. 219-222]. Based on the analyzed scientific publications of Ukrainian researchers, one can find key areas of study of OSINT (Open-Source Intelligence) technologies in Ukraine, as well as a range of specialists and institutions working in this field.

Security and military direction

Specialists in information security, cyber defense, and military intelligence are beginning to play an important role in the study of OSINT tools. For example, authors M.G. Toma and O.V. Vasilova analyze the use of OSINT to record war crimes in Ukraine, in particular in the context of a full-scale invasion of the Russian Federation. Their work has practical significance for documenting violations of international humanitarian law [6]. Yarovoy T. considers the mechanism of obtaining intelligence information from open sources as one of the promising tools for monitoring lobbying activities in the field of ensuring state security [7].

Cybersecurity and digital information hygiene

Another layer of research focused on the impact of OSINT on state cybersecurity. The works of V. Ivkova and I. Opirsky highlight some of the threats associated with open sources and the risks of leakage of critical information [1].

Law and forensics

A separate group of studies focuses on the use of OSINT in criminal law and proving crimes. A. Likhtanska and V. Mykhaylov, in particular, consider open sources as an evidentiary base in legal processes. This direction is promising in view of the integration of OSINT into subsequent actions and activities of law enforcement agencies [3]. OSINT is increasingly being studied in an interdisciplinary context – at the intersection of information technology, law, social sciences and journalism.

The results of the research. A surprising outcome of the study is the number of materials identified, particularly those originating from scientific databases. Precise searching enabled the identification of six items in the Web of Science and Scopus databases. After selecting online media sources, 37 materials were analyzed (see appendices). It should be noted that in this study, the number of sources is not of primary importance, rather, it is their quality, specifically the information regarding journalists’ use of OSINT and AI techniques, that is crucial.

Key observations following the online source search:

1. The materials identified also include processed content, that is, those which do not constitute a primary source (the first created by an editorial team as part of OSINT or AI activities). In processed sources, the actions undertaken by other editorial teams are described. This may result from the difficulties associated with searching the digital content of Ukrainian servers, as primary materials may have been incompletely described in editorial systems (metadata, tags), whereas these secondary sources have been better indexed by search engines.

2. It is important to emphasize that the results indicate tools that were used by journalists directly (when they used them independently) or indirectly. Indirect use means that media outlets could receive partial (raw) or processed (ready-to-use) data from specialized services (such as Molfar, Maltego, and others indicated below), as well as from governmental or military institutions working with OSINT and AI. On this basis, editorial teams created media content and presented the OSINT and AI techniques utilized therein. In the sources found, it is not always possible to unequivocally determine whether journalists worked with applications directly or indirectly.

3. The secondary sources may also have described content from media not published online (i.e., so-called traditional media). This could not be verified during the course of the study.

What is significant is that the results indicate what was used and for what purpose. This also allows for the identification of educational vectors for current and future media professionals

A crucial element in identifying competencies and skills is the recognition of activities undertaken within OSINT and AI frameworks. Some of the most prominent and frequently cited cases include investigative work related to such shocking events as the downing of Malaysian Airlines flight MH-17 (the 2014 disaster), the cluster munition attack on the Kramatorsk railway station, the bombing of the theater in Mariupol marked with the word “Children”, and the search for Russian soldiers involved in torture and the killing of civilians in the Kherson region (events after February 2022). Journalists utilized messengers, especially Telegram, social media platforms, and applications supporting facial recognition in photos and videos.

The tools identified in the sources include:

1. Spreadsheets – used by Bellingcat for inputting links and fact-checking.

2. Social media Telegram, Vkontakte, Odnoklassniki, Flickr – for searching posts, photos, and videos published by soldiers, witnesses, and officials, as well as for identifying Russian soldiers and documenting crimes.

3. Russian databases – often openly available online, containing information such as reports, income, or casino clients, compiled with other open sources.

4. GetContact – for verifying phone number ownership and institutional affiliation.

5. Onlinegibdd.ru and Avtocod.ru – Russian services for vehicle information based on VIN or other data.

6. Rusprofile.ru – Russian platform for legal entity information.

7. Yandex Eda – food and stuff delivery service, for information on individuals' locations or habits.

8. Truly Media and Uwazi – content management systems for organizing and analyzing large datasets.

9. Internet Archive and Archive.today – tools for archiving websites and content.

10. Youtube-dl – open-source software for downloading videos from various platforms.

11. Reverse image search and metadata analysis - fundamental techniques verifying photo authenticity.

12. Google Earth, Google Earth Pro, Open Street Map, Wikimapia, Planet – geospatial analysis and monitoring of military activities or changes in occupied territories.

13. Overpass Turbo – data extraction from Open Street Map.

14. Chronolocation software – determining the time and place of photo or video capture using landmarks, sun position, and shadows of objects.

15. Camopedia – a database of military camouflage and equipment for verifying uniforms in photos.

16. YouControl, TyKhto, and RuAssets – applications using open data to verify individuals and companies (e.g., those connected to Russia or under sanctions).

17. Audio recordings (e.g., intercepted conversations) – used to identify perpetrators and document actions, often combined with other data.

18. General databases – mentioned as sources for information on Russian losses and company connections, including the US SEC database for company verification.

Use of artificial intelligence models:

1. OBRIY system – developed by the Ukrainian group "CyberBoroshno", for automatic collection and analysis of adversary's public materials, filtering and selecting photos and content from public sources.

2. Primer Command – for processing large datasets from enemy radio intercepts, including dialogue summarization, weapon classification, topic identification, and geolocation.

3. Betafaceapi and Cognitec – facial recognition in photos and videos.

4. Invid-project.eu – video search and verification using reverse video search.

Based on the collected sources describing the application of broadly understood OSINT and AI techniques in Ukraine, ten key functionalities were distinguished:

1. Identification and geolocation of military objects: geolocating and correlating targets by determining the place and time of photos and videos published by the adversary.

2. Tracking troop and military equipment movements: based on publicly available materials, such as soldiers' social media photos.

3. Documenting and accounting for war crimes: photographic and video materials shared online, particularly by enemy soldiers and witnesses, for identifying potential perpetrators (e.g., in Bucha, identified through lost phone photos).

4. Information verification and countering disinformation: identifying disinformation, information-psychological operations (IPSO), and false narratives or propaganda from Russian media (fake news, deepfakes).

5. Identification of military personnel and collaborators: advanced searches from multiple correlated sources about Russian military personnel, commanders, and collaborators.

6. Analysis of economic and financial entities: searching for Russian and Belarusian companies, assets, and individuals attempting to circumvent sanctions, countering terrorist financing by Russia. This includes contractor verification in major international projects and analyzing the impact of company operations (e.g., mining) on the environment using GEOINT.

7. Verification of credibility and connections of individuals: analyzing social media activity, photo-based person searches, identity verification, including for sensitive job candidates and public figures.

8. Automated data collection and source monitoring: data gathering and analysis, finding correlations and patterns for automatic object recognition (e.g., in satellite images).

9. Identification of new trends and monitoring public sentiment: tracking reactions to content, detecting social moods, monitoring the activities of influential individuals or organizations.

10. Analysis of hidden connections and pattern modeling: facilitating faster understanding of complex issues, particularly in politics or finance, by correlating seemingly unrelated data.

An important finding is the recognition of Ukrainian sources of OSINT knowledge. The Russian invasion prompted the creation of platforms explaining open-source techniques and organizing numerous training sessions. Some services operate in a specialized manner, offering services free of charge or commercially, providing informational support to journalists and institutions documenting and prosecuting aggressors. These include platforms such as Osintforukraine.com, Molfar.com, Chatovi.online, and foundations with OSINT departments, such as Prytulafoundation.org. International services, such as Oryxspioenkop.com and Maltego.com, have also become involved. Journalistic organizations, e.g. PressAssociation.org.ua, have recognized the growing importance of such online activities, and military services have promoted OSINT courses, e.g., Armyinform.com.ua.

The above findings indicate the necessity of training journalists in the use of technologies supporting OSINT. According to the European Qualifications Framework (EQF) , which sets educational guidelines and required levels of education, a first level degree should demonstrate competencies enabling the management of complex technical or professional activities or projects, and responsibility for decision-making in unpredictable work or learning contexts. At the second level, highly specialized knowledge and problem-solving skills for research or innovative activities are required, as well as the ability to integrate knowledge from various fields. Competencies also include managing and transforming complex, unpredictable work or learning contexts that require new strategic approaches. The tools and functionalities identified in this study closely align with the requirements for the second level degree, where greater emphasis is placed on creating new knowledge, integrating it, and initiating new approaches – skills essential for OSINT or AI use .

Modern activities of Ukrainian media within OSINT correspond to the key areas of digital competence for journalists described in international documents and by specialized research institutions. Notable examples include the Model Curricula for Journalism Education by UNESCO , The 2019 State of Technology in Global Newsroom by the International Center For Journalists , and Predictions 2020 by the Nieman Foundation for Journalism at Harvard University . These documents identify five main categories of competencies: information and data literacy, communication and collaboration, digital content creation, safety, and technical problem-solving. Additionally, knowledge and understanding of changes in the media environment due to digitalization, including the influence of social media, business model evolution, and audience preferences, are crucial. Activities related to OSINT and AI tools are part of the modern digital journalist’s competence framework and should be incorporated into curricula to enable the media to fulfill their role as guardians of truth and credibility.

Introducing OSINT into the educational process of journalists at Sumy State University

In the current context of rapidly evolving digital technologies and increasing information threats, the ability to work with open-source intelligence (OSINT) has become particularly important in the professional training of journalists.

Within journalism education, regional higher education institutions in Ukraine have already begun incorporating OSINT and AI elements into training modules – primarily through partnership projects or teacher-led initiatives. Public organizations also play a key role in this process by conducting regional training sessions and offering free access to analytical tools.

Despite the fragmented introduction of OSINT/AI elements into the journalism curriculum across Ukrainian universities, the Department of Journalism and Philology at Sumy State University has become a flagship in this initiative, purposefully developing these competencies through various educational formats and practical tools integrated into the learning process. Also, OSINT methods are formally introduced as part of the educational components of bachelor's and master's programs in the specialty “Journalism”. Elements of open intelligence are actively used when studying the discipline of media analytics, digital security, fact-checking, journalistic investigations and modern information hygiene.

The practical component of training ensures that students complete tasks related to searching, verifying, and systematizing data from open sources; analyzing social networks; visually monitoring digital content; and studying state content registers and information traces. A key role in this process is played by the department's extensive cooperation with local media, which serve not only as practice bases but also as platforms for student immersion in real media environments where OSINT is actively used for journalistic verification and investigation.

The primary sources of data for conducting OSINT research are social networks – particularly Instagram, Facebook, and TikTok – as well as platforms originating from the Russian Federation, such as VKontakte, Odnoklassniki, and LiveJournal.

Additional categories of open sources include:

- Official state resources (e.g., public reports, declarations, transcripts of press conferences) such as Prozorro, YouControl, and OpenDataBot;
- Traditional and digital media in both print and online formats;
- Academic sources, including scholarly publications, monographs, and professional research;
- “Gray” literature, such as patents, technical reports, and research results not available in mainstream scientific databases;
- Observation data, including radio intercepts, satellite imagery, and aerial photography;
- Commercial information sources, such as images, financial and market analysis, and specialized databases.

In addition to formal education, students actively engage in informal learning through participation in workshops, training sessions, OSINT schools, online courses, and seminars with leading experts and media professionals. This involvement allows them to master up-to-date tools and practices, including those related to the use of artificial intelligence in processing open data.

It is worth noting that the Department of Journalism and Philology at Sumy State University was the first in Ukraine to introduce weekly classes featuring employers and media practitioners who share their real-world experience of working in the information environment. Topics covered in these sessions include the use of OSINT tools, digital databases, social networks, generative technologies, and the principles of responsible use of artificial intelligence in journalism.

Thus, the integration of OSINT training at the Department of Journalism and Philology at Sumy State University ensures a high level of professional preparedness for working under hybrid information threats. It fosters critical thinking, digital media literacy, and the ability to analyze and interpret data from open sources.

Conclusions and prospects. An important result of the study is the identification of a limited number of scientific publications. Thus, the authors addresse cognitive gap in access to this type of research. The scarcity of such studies can be interpreted as an indication for scholars, including those from Ukraine, to fill this gap by writing about OSINT technologies and artificial intelligence as crucial tools for data verification during war or crisis situations. Publishing in journals indexed in international databases would allow for a better understanding of Ukrainian journalism in times of armed conflict, its challenges and needs, as well as the dangers associated with hostile wartime propaganda. This constitutes an educational vector for researchers, academics, and educators.

It is worth emphasizing that the study revealed improper indexing (metadata description) of many valuable sources concerning the activities of Ukrainian media within OSINT and AI frameworks. As a result, accessing and verifying their reliability proved difficult. Proper assignment of keywords and tagging in online systems would improve their visibility on the internet, potentially influencing the global perception of the war. It should also be stressed that content ought to be thoroughly documented, primarily with official reports, so that media coverage can be recognized as informative rather than propagandistic. This highlights the need for technical knowledge related to constructing online communications.

The analysis of Ukrainian sources and the experiences of journalists and media professionals clearly indicates that in the environment of modern technologies, a person becomes a “sensor” who can be detected and tracked. This underscores the necessity of technological education not only for future but also current journalists. OSINT and artificial intelligence tools require digital competencies that add new value to reporting, enable source authentication, fact documentation, tracking false information, and detecting hostile activity. They should be implemented in the curricula so that the media can act as a guardian of truth and credibility. Even if a journalist does not directly use OSINT or AI tools, he should know their effectiveness and understand the effect obtained. The Ukrainian example – media engagement with technology and its skillful use on the “media battlefield”, can serve as a model for a modern, credible and reliable journalistic practice.

Despite significant progress, the development of OSINT in Ukraine still requires institutionalization, methodological support, ethical frameworks, and sustained state backing. At the same time, the ongoing war continues to drive the evolution of digital journalism – and, with it, the deeper exploration of OSINT. There is a growing need to establish a national OSINT platform that includes educational, journalistic, and analytical components. In the future, OSINT should become a mandatory component of professional journalism standards, particularly critical in an era of fake news, generative technologies, and new forms of informational warfare.

Currently, the integration of OSINT technologies into educational programs remains uneven. Several challenges persist: a shortage of specialists capable of teaching across media, technology, and analytics; a lack of integrated courses (with most offerings limited to electives or individual initiatives); insufficient funding; and inadequate infrastructure for storing and processing large volumes of data.

OSINT is not merely a new tool for journalists – it is a transformational factor reshaping the media profession and the structure of media education. In Ukraine’s wartime context, marked by hybrid information threats, OSINT is a strategic asset. The geographic proximity of the Sumy region to the frontline makes it particularly vulnerable to information aggression, increasing the demand for high-quality OSINT approaches and automated fact-checking systems.

1. Ivkova, V., and Opirskyi, I. (2025). *OSINT-tekhnolohii yak zahroza kiberbezpetsi derzhavy* [OSINT technologies as a threat to state cybersecurity]. *Kiberbezpeka: osvita, nauka, tekhnika*, 3(27), 165–179. DOI: https://doi.org/10.28925/2663-4023.2025.27.749.

2. Kopotun, I., Koropatnik, I., and Mykytiuk, M. (2024). *Viiskova zhurnalistyka. Ukrainskyi aspekt. Stanovlennia ukrainskoi viiskovoi zhurnalistyky* [Military journalism. The Ukrainian aspect. Formation of Ukrainian military journalism]. Kyiv: [b. v.]. ISBN 978-611-0129-28-2.

3. Likhtanska, A. P., and Mykhailov, V. O. (2024). *Vykorystannia OSINT v kryminalnomu pravi Ukrainy* [The use of OSINT in the criminal law of Ukraine]. *DICTUM FACTUM*, 1(15), 105–111. DOI: https://doi.org/10.32703/2663-6352/2024-1-15-105-111.

4. Maliienko, A., Yakovets, A., and Bondar, Yu. (2022). *Zhurnalisty na viini. Dokumentalni doslidzhennia, khronikalnyi litopys, analityka* [Journalists at war: Documentary studies, chronicle, analytics]. Kharkiv: [b. v.]. ISBN 978-617-551-122-0.

5. Maliienko, A., Yakovets, A., and Bondar, Yu. (2023). *Ukraina. Zhurnalisty na peredovii. Zbirka narysiv i statei* [Ukraine. Journalists on the frontline: A collection of essays and articles]. Kyiv: [b. v.]. ISBN 978-617-8259-28-0.

6. Toma, M. H., and Vasylova, O. V. (2025). *Instrumenty OSINT: fiksatsiia voiennykh zlochyniv v Ukraini* [OSINT tools: recording war crimes in Ukraine]. *Zhurnal polityky, prava ta sotsialnykh aktualnykh pytan*, 2, 905–909. DOI: https://doi.org/10.24144/2788-6018.2025.02.134.

7. Yarovyi, T. S. (2019). *OSINT yak perspektyvnyi instrument kontroliu za lobistskoiu diialnistiu v konteksti derzhavnoi bezpeky* [OSINT as a promising tool for monitoring lobbying activities in the context of state security]. *Ekspert: paradyhmy yurydychnykh nauk i derzhavnoho upravlinnia*, 4(6), 201–208. DOI: https://doi.org/10.32689/2617-9660-2019-4(6)-201-208.

8. A Handbook for Journalism Educators. *Reporting on Artificial Intelligence* / Ed. by M. Jaakkola. (2023). Paris: UNESCO, pp. 27–36. ISBN 978-92-3-100592-3. DOI: https://doi.org/10.58338/HSMK8605.

9. Berkeley Protocol on Digital Open Source Investigations: A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law. (2022). Retrieved from https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source (Accessed: 5 November 2025).

10. Block, L. (2023). The long history of OSINT. *Journal of Intelligence History*, 23(2), 95–109. DOI: https://doi.org/10.1080/16161262.2023.2224091.

11. Dierickx, L., and Lindén, C. (2024). Screens as battlefields: Fact-checkers' multidimensional challenges in debunking Russian-Ukrainian war propaganda. *Media and Communication*, 12, Article 8668. DOI: https://doi.org/10.17645/mac.8668.

12. García-Marín, D., and Salvat-Martinrey, G. (2023). Desinformación y guerra. Verificación de las imágenes falsas sobre el conflicto ruso-ucraniano. *ICONO 14. Revista Científica de Comunicación y Tecnologías Emergentes*, 21(1). DOI: https://doi.org/10.7195/ri14.v21i1.1943.

13. Ghioni, R., Taddeo, M., and Floridi, L. (2024). Open source intelligence and AI: a systematic review of the GELSI literature. *AI & Society*, 39, 1827–1842. DOI: https://doi.org/10.1007/s00146-023-01628-x.

14. Hwang, Y.-W., Lee, I.-Y., Kim, H., Lee, H., and Kim, D. (2022). Current status and security trend of OSINT. *Wireless Communications and Mobile Computing*, Article ID 1290129, 14 p. DOI: https://doi.org/10.1155/2022/1290129.

15. Khan, S. A., Dierickx, L., Furuly, J.-G., Vold, H. B., Tahseen, R., Linden, C.-G., and Dang-Nguyen, D.-T. (2025). Debunking war information disorder: A case study in assessing the use of multimedia verification tools. *Journal of the Association for Information Science and Technology*, 76(5), 752–769. DOI: https://doi.org/10.1002/asi.24970.

16. Magallón-Rosa, R., Fernández-Castrillo, C., and Garriga, M. (2023). Fact-checking in war: Types of hoaxes and trends from a year of disinformation in the Russo-Ukrainian war. *Profesional de la información*, 32(5), e320520. DOI: https://doi.org/10.3145/epi.2023.sep.20.

17. Morejón-Llamas, N., Martín-Ramallal, P., and Micaletto-Belda, J.-P. (2022). Twitter content curation as an antidote to hybrid warfare during Russia's invasion of Ukraine. *Profesional de la información*, 31(3), e310308. DOI: https://doi.org/10.3145/epi.2022.may.08.

18. Nissen, I. A., Walter, J. G., Charquero-Ballester, M., and Bechmann, A. (2022). Digital infrastructures of COVID-19 misinformation: A new conceptual and analytical perspective on fact-checking. *Digital Journalism*. Retrieved from https://www.tandfonline.com/journals/rdij20 (Accessed: 5 November 2025).

19. Zecchinon, P., and Standaert, O. (2025). The war in Ukraine through the prism of visual disinformation and the limits of specialized fact-checking: A case study at *Le Monde*. *Digital Journalism*, 13(1), 61–79. DOI: https://doi.org/10.1080/21670811.2024.2332609.

20. Schapals, A. K., and Bruns, A. (2022). *Media and Communication*, 10(3), 5–16. DOI: https://doi.org/10.17645/mac.v10i3.5401.

21. Wohlin, C. (2014). Guidelines for snowballing in systematic literature studies and a replication in software engineering. In *Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering (EASE '14)*. New York: Association for Computing Machinery, Article 38, pp. 1–10. DOI: https://doi.org/10.1145/2601248.2601268.

УДК 007 : 304 : 659.3

ВІЙНА В УКРАЇНІ: ПІДГОТОВКА ЖУРНАЛІСТІВ ДО РОБОТИ В КРИЗОВИХ УМОВАХ

Ковалик Кшиштоф[1], доктор габілітований,
ORCID – https://orcid.org/0000-0001-8511-6851;
Ляшенко Ірина[2]**,** кандидат педагогічних наук, доцент,
ORCID – https://orcid.org/0000-0003-4211-5116;
Бондаренко Олена[2,3], кандидат філологічних наук, доцент,
ORCID – https://orcid.org/0000-0002-2369-774X.
[1] Варшавський університет, Польща,
[2] Сумський державний університет, Україна.
[3] Кореспондентний автор Бондаренко О., e-mail: ol.bondarenko@journ.sumdu.edu.ua

Стаття надійшла до редакції 10.08.2025 р.
Надіслано після редагування 10.09.2025 р.
Рекомендовано до видання 06.11.2025 р.

Цитування: *Ковалик, К., Ляшенко, І., Бондаренко, О. (2025). Війна в Україні: підготовка журналістів до роботи в кризових умовах. Образ, 3 (49), 6–17. https://doi.org/10.21272/Obraz.2025.3(49)-6-17.*

Вступ. У статті проаналізовано виклики та нові компетентності, яких потребують журналісти, що висвітлюють війну в Україні з 2022 року, акцентовано увагу на роль цифрових технологій, інструментів OSINT (розвідки на основі відкритих джерел) та генеративного штучного інтелекту.

Актуальність дослідження. В умовах повномасштабної війни українські медіа зіткнулися з необхідністю не лише забезпечувати суспільство достовірною інформацією та протидіяти дезінформації, а й оперативно адаптовуватися до нових загроз – пропаганда, фейкові новини та діпфейки.

Методологія. Дослідження ґрунтується на аналізі кейсів діяльності українських журналістів, застосуванні цифрових інструментів верифікації, а також на огляді наукової літератури та медіаматеріалів за 2022–2025 роки. Для визначення каталогу найважливіших інструментів і компетентностей, необхідних у роботі журналіста в умовах війни, використано розширені техніки пошуку та аналітичні інструменти PinPoint і Notebook LM.

Результати. Отримані результати свідчать, що ключовими навичками є робота з відкритими джерелами, аналіз даних, фактчекінг та володіння інструментами штучного інтелекту – із дотриманням принципів етики та інформаційної безпеки.

Висновки. Досвід українських медіа підкреслює необхідність безперервної освіти журналістів у сфері новітніх технологій і розвитку стійкості до інформаційного та психологічного тиску з боку противника. У статті сформульовано рекомендації для журналістської освіти, зокрема – щодо розроблення каталогу цифрових інструментів і компетентностей, які дадуть змогу медіа зберігати стандарти достовірності та надійності під час криз.

Ключові слова: *медіа, журналістика, Україна, війна, освіта, кризи, OSINT, штучний інтелект, технології.*

1. kova, V., and Opirskyi, I. (2025). *OSINT-tekhnolohii yak zahroza kiberbezpetsi derzhavy* [OSINT technologies as a threat to state cybersecurity]. *Kiberbezpeka: osvita, nauka, tekhnika*, 3(27), 165–179. DOI: https://doi.org/10.28925/2663-4023.2025.27.749.
2. Kopotun, I., Koropatnik, I., and Mykytiuk, M. (2024). *Viiskova zhurnalistyka. Ukrainskyi aspekt. Stanovlennia ukrainskoi viiskovoi zhurnalistyky* [Military journalism. The Ukrainian aspect. Formation of Ukrainian military journalism]. Kyiv: [b. v.]. ISBN 978-611-0129-28-2.
3. Likhtanska, A. P., and Mykhailov, V. O. (2024). *Vykorystannia OSINT v kryminalnomu pravi Ukrainy* [The use of OSINT in the criminal law of Ukraine]. *DICTUM FACTUM*, 1(15), 105–111. DOI: https://doi.org/10.32703/2663-6352/2024-1-15-105-111.
4. Maliienko, A., Yakovets, A., and Bondar, Yu. (2022). *Zhurnalisty na viini. Dokumentalni*

doslidzhennia, khronikalnyi litopys, analityka [Journalists at war: Documentary studies, chronicle, analytics]. Kharkiv: [b. v.]. ISBN 978-617-551-122-0.

5. Maliienko, A., Yakovets, A., and Bondar, Yu. (2023). *Ukraina. Zhurnalisty na peredovii. Zbirka narysiv i statei* [Ukraine. Journalists on the frontline: A collection of essays and articles]. Kyiv: [b. v.]. ISBN 978-617-8259-28-0.

6. Toma, M. H., and Vasylova, O. V. (2025). *Instrumenty OSINT: fiksatsiia voiennykh zlochyniv v Ukraini* [OSINT tools: recording war crimes in Ukraine]. *Zhurnal polityky, prava ta sotsialnykh aktualnykh pytan*, 2, 905–909. DOI: https://doi.org/10.24144/2788-6018.2025.02.134.

7. Yarovyi, T. S. (2019). *OSINT yak perspektyvnyi instrument kontroliu za lobistskoiu diialnistiu v konteksti derzhavnoi bezpeky* [OSINT as a promising tool for monitoring lobbying activities in the context of state security]. *Ekspert: paradyhmy yurydychnykh nauk i derzhavnoho upravlinnia*, 4(6), 201–208. DOI: https://doi.org/10.32689/2617-9660-2019-4(6)-201-208.

8. A Handbook for Journalism Educators. *Reporting on Artificial Intelligence* / Ed. by M. Jaakkola. (2023). Paris: UNESCO, pp. 27–36. ISBN 978-92-3-100592-3. DOI: https://doi.org/10.58338/HSMK8605.

9. Berkeley Protocol on Digital Open Source Investigations: A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law. (2022). Retrieved from https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source (Accessed: 5 November 2025).

10. Block, L. (2023). The long history of OSINT. *Journal of Intelligence History*, 23(2), 95–109. DOI: https://doi.org/10.1080/16161262.2023.2224091.

11. Dierickx, L., and Lindén, C. (2024). Screens as battlefields: Fact-checkers' multidimensional challenges in debunking Russian-Ukrainian war propaganda. *Media and Communication*, 12, Article 8668. DOI: https://doi.org/10.17645/mac.8668.

12. García-Marín, D., and Salvat-Martinrey, G. (2023). Desinformación y guerra. Verificación de las imágenes falsas sobre el conflicto ruso-ucraniano. *ICONO 14. Revista Científica de Comunicación y Tecnologías Emergentes*, 21(1). DOI: https://doi.org/10.7195/ri14.v21i1.1943.

13. Ghioni, R., Taddeo, M., and Floridi, L. (2024). Open source intelligence and AI: a systematic review of the GELSI literature. *AI & Society*, 39, 1827–1842. DOI: https://doi.org/10.1007/s00146-023-01628-x.

14. Hwang, Y.-W., Lee, I.-Y., Kim, H., Lee, H., and Kim, D. (2022). Current status and security trend of OSINT. *Wireless Communications and Mobile Computing*, Article ID 1290129, 14 p. DOI: https://doi.org/10.1155/2022/1290129.

15. Khan, S. A., Dierickx, L., Furuly, J.-G., Vold, H. B., Tahseen, R., Linden, C.-G., and Dang-Nguyen, D.-T. (2025). Debunking war information disorder: A case study in assessing the use of multimedia verification tools. *Journal of the Association for Information Science and Technology*, 76(5), 752–769. DOI: https://doi.org/10.1002/asi.24970.

16. Magallón-Rosa, R., Fernández-Castrillo, C., and Garriga, M. (2023). Fact-checking in war: Types of hoaxes and trends from a year of disinformation in the Russo-Ukrainian war. *Profesional de la información*, 32(5), e320520. DOI: https://doi.org/10.3145/epi.2023.sep.20.

17. Morejón-Llamas, N., Martín-Ramallal, P., and Micaletto-Belda, J.-P. (2022). Twitter content curation as an antidote to hybrid warfare during Russia's invasion of Ukraine. *Profesional de la información*, 31(3), e310308. DOI: https://doi.org/10.3145/epi.2022.may.08.

18. Nissen, I. A., Walter, J. G., Charquero-Ballester, M., and Bechmann, A. (2022). Digital infrastructures of COVID-19 misinformation: A new conceptual and analytical perspective on fact-checking. *Digital Journalism*. Retrieved from https://www.tandfonline.com/journals/rdij20 (Accessed: 5 November 2025).

19. Zecchinon, P., and Standaert, O. (2025). The war in Ukraine through the prism of visual disinformation and the limits of specialized fact-checking: A case study at *Le Monde*. *Digital Journalism*, 13(1), 61–79. DOI: https://doi.org/10.1080/21670811.2024.2332609.

20. Schapals, A. K., and Bruns, A. (2022). *Media and Communication*, 10(3), 5–16. DOI: https://doi.org/10.17645/mac.v10i3.5401.

21. Wohlin, C. (2014). Guidelines for snowballing in systematic literature studies and a replication in software engineering. In *Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering (EASE '14)*. New York: Association for Computing Machinery, Article 38, pp. 1–10. DOI: https://doi.org/10.1145/2601248.2601268.