Society. Document. Communication

Journal homepage: https://sdc-journal.com.ua/en
Society. Document. Communication, Vol. 11, No. 2, 84-97

Article's History: Received: 17.12.2025 Revised: 15.04.2026 Accepted: 12.05.2026 Published: 30.05.2026

UDC 930.25:004:341.3(477)
DOI: 10.69587/sdc/2.2026.84

ISSN 2518-7600
e-ISSN 2524-1060

Military documentation as a source of historical memory: Problems of preserving digital evidence of the war in Ukraine

Alla Zlenko*
PhD in History, Professor
Hryhorii Skovoroda University in Pereiaslav
08401, 30 Sukhomlynskyi Str., Pereiaslav, Ukraine
https://orcid.org/0000-0002-5586-3984
Yurii Liashchenko
Lecturer
Hryhorii Skovoroda University in Pereiaslav
08401, 30 Sukhomlynskyi Str., Pereiaslav, Ukraine
https://orcid.org/0009-0007-1302-6823
Nadiia Riznyk
Lecturer
Hryhorii Skovoroda University in Pereiaslav
08401, 30 Sukhomlynskyi Str., Pereiaslav, Ukraine
https://orcid.org/0000-0003-0893-9795

Abstract. The purpose of the study was to analyse the role of military documentation in the construction of historical and social memory and to investigate specific challenges associated with the preservation of digital evidence of the war in Ukraine. A comprehensive interdisciplinary approach was applied, which through regulatory, document, comparative, and content analysis covered legislative acts, institutional practices, archival projects, digital platforms, and open-source materials, which allowed tracing the mechanisms of creating, storing, verifying, and using digital evidence of war. In the course of the study, it was found that digital military documentation was transformed from an auxiliary information resource into a central element of war documentation, simultaneously acquiring evidence, memorial, and communicative significance. It was revealed that a full-scale war led to the development of one of the world's largest arrays of digital evidence, which includes official documents, multimedia materials, satellite images, and eyewitness accounts. The functional complementarity of various types of digital documentation was revealed, where state archives provide legal legitimation, and public and media initiatives – efficiency and social representation of events. Analysis of the regulatory framework revealed gaps in the procedural regulation of the status of digital evidence, which led to inconsistencies in law enforcement practices. The study of institutional practices showed progress in the scale of digitisation of archival funds, simultaneously identifying the problem of fragmentation of storage standards and metadata. Separately, it was proved that the spread of digital content manipulation technologies has actualised the need to introduce complex verification procedures and international evidence evaluation protocols. It was concluded that the effective preservation and use of digital military documentation is possible only if state, public, and international institutions coordinate based on unified

Suggested Citation:
Zlenko, A., Liashchenko, Yu., & Riznyk, N. (2026). Military documentation as a source of historical memory: Problems of preserving digital evidence of the war in Ukraine. *Society. Document. Communication*, 11(2), 84-97. doi: 10.69587/sdc/2.2026.84.

*Corresponding author (zlenko.am@ukr.net)

legal, technical, and ethical standards. The results of the study will be of interest to archivists, lawyers, researchers in the humanities, journalists, and specialists in documenting war crimes who work with digital evidence of war and the development of historical and collective memory

Keywords: archives; multimedia materials; eyewitness accounts; disinformation; crimes

Introduction

The relevance of the topic of military documentation as a source of historical memory is determined by the unprecedented intensity and scale of digital recording of the full-scale invasion of Ukraine by the Russian Federation, which began in 2022. The course of military events is accompanied by the mass production of digital evidence in the form of official documents, satellite images, video and photo materials, OSINT data (Open-source intelligence), journalistic reports and eyewitness accounts, which simultaneously serve as evidence of war crimes, sources of historical knowledge and carriers of collective memory. In the digital age, military documentation is gradually losing its status as an auxiliary tool of historiography and is transformed into a complex multidimensional system located at the intersection of archival studies, media research, digital humanities, international law, and memorial studies. The issue of preservation, authentication, and long-term use of digital evidence is aggravated by the destruction of infrastructure, algorithmic policies of digital platforms, legal uncertainty, and threats of content manipulation, which calls into question their stability as a historical source and legally permissible evidence.

Within the scientific discourse, digital military documentation was interpreted in several interrelated analytical planes. In particular, B. Christensen & A. Khalil (2023) focused on the transformation of conflict journalism under the influence of digital technologies and social media, exploring journalists' use of platforms X, encrypted messengers, and other digital tools to collect, verify, and disseminate information from war zones. Their analysis showed that digital affordances allowed combining source security, efficiency, and professional standards, while strengthening the role of journalists as mediators between war events and public interpretation. As a result, the researchers emphasised the importance of digital materials not only as a news product, but also as a potential historical and evidence-based resource. Another dimension of the problem was revealed in the study by M. Ochi & H. Dagenborg (2025), who conducted a systematic analysis of 52 online war crimes archives and classified them into evidence archives, legal material archives, and memory archives. The paper noted that the technical complexity of digital archives remained opaque to lawyers, reducing the effectiveness of their use in legal proceedings and increasing data security risks. The principles of "do no harm" and "efficiency" proposed by the researchers were justified as basic for designing digital archives, which allowed consolidating the idea of them as a tool for combining justice, historical accuracy, and collective memory. The problems of using advanced technologies in the context of the prosecution of war crimes of the Russian Federation in Ukraine were considered in the paper by M.S. Ellis (2025). The researcher reasoned the critical role of digital evidence in conflicts and outlined the unique position of Ukraine as an active subject of global justice. The conclusion that the effectiveness of digital documentation depends on international solidarity and institutional support allowed interpreting it not only as a tool for recording it, but also as an element of global political and legal interaction.

In parallel with the legal aspects, the research focused on the preservation of cultural heritage in war conditions. concrete example of civic engagement in digital heritage preservation was presented in the paper by A.A. da Costa & L.R.M. Santos (2023), dedicated to the Backup Ukraine Project. The researchers demonstrated that using the Polycam application and involving citizens in creating 3D copies of cultural objects transformed the passive position of the population into a form of active participation in heritage preservation, confirming that even in conditions of instability and resource scarcity, digital documentation remains effective through the active involvement of local communities and the use of open tools. Thus, the combination of digital technologies, the concept of "soft power" and collective memory practices formed a new model of responsibility, in which individual digital actions acquired national and historical significance. S. Bonjack (2025) examined the genesis and success of the SUCHO (Saving Ukrainian Cultural Heritage Online) initiative as a model for mass rescue of digital cultural heritage during the war. The researcher analysed the role of professional communities and personal connections in responding to conflicts and suggested creating structured teams to save data in the context of military operations. M. Gentile (2025) explored the process of memorialising the war of independence of Ukraine in the context of nation-building during a full-scale Russian invasion. The researcher analysed six urban places of memory, finding that the military nation is based on the connection with past challenges for the nation, the definition of Ukraine as the antithesis of Russia, the marginalisation of the Soviet past, and the mobilisation of local identity. The study by D. Vonnák *et al.* (2025) analysed transnational networks and practices of mobilising aid for the protection of Ukraine's cultural heritage during a full-scale war. The study identified actors, resources, logistics chains, and organisational alliances, and analysed intersections between extreme

cultural and humanitarian responses, pointing to factors that contribute to or hinder effective coordination of aid on the ground. The study by M. Bareikytė & M. Makhortykh (2024) was aimed at analysing the transformation of the practice of witnessing war on digital platforms using the example of a Telegram channel dedicated to the occupied Ukrainian city. The researchers empirically investigated inconspicuous digital evidence as a non-institutionalised form, identifying changes in communication practices during different periods of occupation and substantiating the concept of digitally accessible evidence of war considering its polyvocality.

Despite the amount of research, the comprehensive understanding of military documentation as an integrated source of historical and social memory through the prism of the problems of preserving digital evidence of war remained insufficiently systematised. The purpose of the study was to investigate military documentation as a source of development of historical and social memory and to outline the problems of preserving digital evidence of the war in Ukraine. To achieve this goal, it was planned to classify the main types of digital evidence of war, analyse the challenges of their preservation and verification in the context of armed conflict, and determine the importance of military documentation for social communication and the processes of forming collective memory.

Materials and Methods

The methodological structure of the study was based on a comprehensive multidimensional approach aimed at a comprehensive investigation of the phenomenon of digital military documentation in Ukraine as a complex object located at the intersection of legal, archival, communication, and memorial practices. To achieve this goal, an interrelated set of methods focused on the collection, systematisation, comparative analysis, and interpretation of heterogeneous sources and data was applied, which allowed considering the subject of research from an integrated perspective. The regulatory framework for the study was established through a critical analysis of national legislation. The study focused on the Criminal Procedure Code of Ukraine (2012), with an emphasis on identifying existing definitions, procedural rules, and gaps relating to the regulation of the status, collection, recording, and assessment of digital (electronic) evidence. The official profile of Ukraine in the Budapest Convention on Cybercrime (Council of Europe, 2022) was used to contextualise national approaches within the international framework and determine basic eligibility criteria. Simultaneously, analytical materials contained within the CyberUA project initiated by the Council of Europe (Council of Europe Office in Ukraine, n.d.) were reviewed to analyse areas for institutional capacity development.

Systematisation and classification of digital military documentation arrays were carried out using the document management method and the typological classification method. To characterise the infrastructure component of access to archival heritage, the functionality and significance of an Interarchive Search Portal (State Archival Service of Ukraine, n.d.) was studied. To supplement the public sector, materials from the Ministry of Digital Transformation of Ukraine (2024; n.d.) were used, concerning the creation of a centralised digital archive of documents from the war period, including information about the activities of museums, in particular, the digital collections of the Dovzhenko Centre (n.d.). The study analysed materials that include publications in the media that record Ukraine's achievements in the international context (Ukraine has become..., 2024), and information on specific regional archival initiatives (The Lviv archive..., 2024). The analysis of the public and media documentation contour was carried out using open source analysis methods. In this context, the object of study was the evidence collection tool – the "eVorog" chatbot (Ministry of Digital Transformation of Ukraine, n.d.), and publicly available statistics on the volume and dynamics of its use, reflected in display messages (Ukrinform, 2025). The role of social platforms Facebook (Meta Platforms, Inc., n.d.), Telegram (Telegram Messenger LLP, n.d.) and X (X Corp., n.d.) was considered as technological and communicative environments where digital evidence is generated, archived, circulated and socially reinterpreted, and subsequently incorporated into narratives of collective memory. Specialised materials from the law enforcement and training systems were used to investigate the procedural, expert, and judicial aspects of working with digital evidence. The analysis covered official publications of the Judiciary of Ukraine (2025) devoted to practical aspects of using OSINT materials in criminal proceedings, and analytical developments of the National School of Judges of Ukraine (2025), which contain recommendations on standards for the assessment of digital evidence with reference to international protocols, in particular the Berkeley Protocol. The international legal context was provided through the study of the principles and practices of the International Criminal Court (n.d.), and a critical analysis of expert assessments presented in studies by reputable think tanks, such as the Royal United Services Institute (RUSI) (2024).

The study covered the chronological period of full-scale war from 2022 to 2025, which allowed tracing the dynamics of the development of institutional practices, technological solutions, and social responses to the challenges of this stage. The choice of specific examples (for example, certain archival projects, platforms or tools) was determined by their representativeness, public significance, and illustrative potential for demonstrating trends, achievements, and systemic problems in the field of digital documentation of the war in Ukraine. The material basis of the empirical research was a body of digital military documents and publications selected for content analysis from open, verified, and institutionally relevant sources used in humanitarian, legal, and media studies of the war in Ukraine. The sample included 124

texts published in 2022-2025. The main source of digital military documentation was archival platforms and specialised repositories, in particular the Ukraine War Archive (UWA, n.d.). The group of official documents and public reports that were included in the empirical sample consisted of regulatory materials, reports of monitoring missions, and daily combat reports published by state bodies of Ukraine and international institutions which directly recorded events and actions related to the war. For example, the data from Office of the United Nations High Commissioner for Human Rights (n.d.); international reports of the U.S. Department of State (2025). These materials, united by a common focus on the events of the war, were used in content analysis to compare the content of digital military documents with normative and internationally recognised information about the course of hostilities and human rights violations.

The third group consisted of OSINT data and eyewitness accounts recorded in social networks, digital archives, and instant messengers, which had clear time and geographical markers and were used in reports of human rights organisations or journalistic investigations. Verification of such materials was based on international OSINT research standards, in particular the Berkeley Protocol on Digital Open Source Investigations (National School of Judges of Ukraine, 2025), which set standards for the collection, analysis, and storage of digital data suitable for international legal processes. The inclusion criteria were the presence of a clear temporal and spatial reference, the identified source of origin, the possibility of verifying the material, and its potential suitability for legal or analytical use. The key categories of analysis included: "war crimes", "type of digital evidence", "source of recording", "OSINT verification", "legal relevance", "narrative of testimony", "institutional status of the material". The unit of analysis was defined as a separate document or publication as a whole, with additional micro-level coding of meaningful text fragments (paragraphs and sentences) containing a description of an event, a qualification of an action, or a reference to evidence. This approach combined quantitative comparison of category frequencies with qualitative interpretation of content. The analysis procedure involved a step-by-step selection of materials based on keywords and thematic markers in the sources. Coding was performed using a combined method with NVivo 14 qualitative text analysis software, which ensured the reproducibility of the procedure and transparency of categorisation. To verify the reliability of the encoding, double independent encoding was applied by two researchers, followed by the calculation of Cohen's kappa agreement coefficient, which was $\kappa = 0.81$, corresponding to a high level of inter-encoder reliability according to established methodological criteria. The comparative legal method was used to compare the provisions of national legislation with international standards. The logic of the methodological presentation was built consistently: from the analysis of the regulatory framework and institutional landscape – through the systematisation of types of documentation and the analysis of mechanisms for their creation – to the investigation of technical, procedural, and ethical challenges of their preservation, verification, and use.

Results and Discussion

Military documentation in the system of historical and social memory

Military documentation in humanitarian disciplines is considered as a set of tangible and intangible digital information carriers that record and communicate events and consequences of armed conflicts. In terms of subject matter, it is located at the intersection of historiography, archival and memorial studies, and digital humanities, which allows interpreting it not only as a factual data set, but also as a semiotic complex of conflict memory that forms collective narratives and social identity. The war in Ukraine has become one of the most documented in the digital environment, as millions of photos, videos, audio materials, and messages create a large array of primary digital sources of historical, legal, and cultural significance for future generations (Hoskins & Shchelin, 2023). This data becomes the basis for scientific analysis, legal investigations, and cultural reconstructions of the conflict, for example, the Ukraine War Archive (n.d.) project has collected more than 37 million digital files, including videos, photos, and eyewitness accounts.

In the humanities and legal science of the 21st century, the concept of "document" is considered as a fixed trace of activity and intellectual information that has signs of authenticity, and stores information about a fact, process, or state that can be reproduced in the future (Pédauque, 2022). The document includes information and material components, covering both conventional written media and digital forms, in particular, digital files or databases. This definition emphasises the totality of characteristics of a document as an information resource, including the characteristics of reliability, integrity, and reproducibility, which is the subject of archival science and document management (Lytvynska, 2014). In jurisprudence and criminal procedure, the concept of "evidence" is supplemented by criteria of admissibility, relevance and reliability, which determine whether information can be used in court proceedings. Digital (electronic) evidence in criminal proceedings is electronic information obtained in accordance with procedural legislation that is relevant for establishing the circumstances of the case and can be admitted as evidence. To do this, it is necessary to ensure the authenticity of the data, the ability to establish its origin, time, geographical labels, and compliance with the procedure for extracting and storing it (Ragni, 2023).

In the humanities, in particular in memory studies, digital data is considered as structural units of social memory that not only capture information, but also influence the storage and translation of collective ideas

about the past. Digital archives, social media, and other digital platforms create dynamic collections of materials that influence ways of remembering in society, in particular, by expanding access to historical materials, democratising the creation of narratives and involving social groups in the process of memory documentation. Digital archives and social media function as active environments that change the dynamics of collective memory, including mobility, procedurality, and participation of broad communities in memory practices (Mandolessi, 2024). In the context of the war in Ukraine (2022-2025), the classification of digital evidence reflects different levels of origin, purpose, and functions of data, which allows systematising their contribution to documenting events, evaluating facts, and forming a collective memory of the conflict. This classification is necessary because different types of digital sources have different legal force, different requirements for the collection and storage procedure, and different influences on public perception of war events. The main categories of digital military evidence and their functions in documentation are shown in Table 1.

Table 1. Classification of types of digital military documentation and their functions

Digital evidence category	Main examples of sources	Functions in documenting war	Analytical value
Official government documents	Decrees, orders, registers of victims, state reports	Recording administrative facts, legitimising events, creating a legal basis	Serves as a legally significant base for international litigation and defines data processing standards
Digital archives and databases	Ukraine War Archive, archives of scientific and museum institutions	Centralised storage, structured metadata system, long-term storage	Ensures the reliability and availability of data for scientific research and event reproduction
Multimedia materials	Photo, video recording, satellite images	Visual chronology of events, documentation of destruction and crimes	Allows visual reconstruction of circumstances and confirmation of facts, in particular in forensic examinations
Eyewitness accounts and OSINT	Social networks, personal digital diaries	Personal experiences, context of events, operational reports	Expands understanding of the war experience by creating a dynamic array of social memory

Source: compiled by the authors based on C. Oxendine (2022), S. Mandolessi (2024), G. Chlevickaitė (2025), Judiciary of Ukraine (2025), UWA (n.d.)

This classification demonstrates the structural relationships between different forms of digital sources and their functional roles. Official documents provide legal and administrative record of facts, which makes them necessary for international legal mechanisms, since they are standardised for long-term preservation and have clearly defined time, geographical and identification attributes necessary for procedural use. Digital archives and databases systematise this broad field of data, enabling researchers and human rights defenders to structure and analyse arrays of materials covering various aspects of conflict. Multimedia materials provide a visual component of cognition of events that take place for the reconstruction of circumstances and confirmation of facts in forensic and historical research. Eyewitness accounts and OSINT data expand the field of memory, providing contextual and individual perspectives that are needed to explore the collective memory and social identity of a war-torn society.

Digital archives and databases that arise as a result of cooperation between scientists, human rights organisations, and international institutions serve as a centralised repository with the ability to effectively search and describe metadata. For example, Ukraine War Archive (n.d.) is a platform that combines tens of millions of files, including interviews, photos and videos, and provides a rigorous methodological description and metadata for each material, allowing them to be used as an object of historical and legal research. Other digital archives, such as library and museum initiatives, complement this structure by preserving local and regional documentary collections with a similar goal of making them accessible for scientific analysis and educational projects (Ministry of Digital Transformation of Ukraine, 2024). Multimedia materials, in turn, include visual and audio evidence of events, which usually contain a high level of tactical information – for example, photos of destruction, video recordings of attacks, and satellite images of front lines. Such data is of great importance not only for reconstructing the chronology of events, but also for visually demonstrating facts during judicial and journalistic investigations. OSINT research has demonstrated the effectiveness of algorithmic approaches to verifying such materials, in particular, using geolocation and time markers, which increases their reliability and representativeness as sources of science and law (Khan *et al*., 2023).

Eyewitness accounts and OSINT materials are inherently personalised and contextualised: they reflect individual experiences of war, which is valuable for memory studies. This data appears in social networks and instant messengers, and while its original form may be less structured, digital capture techniques allow metadata and verification to increase its value as evidence or historical sources. A general analysis of the above classification shows that different categories of digital sources complement each other: official documents consolidate

legal and administrative aspects, digital archives provide reliability and long-term preservation, multimedia materials provide visual context, and OSINT evidence expands the contextual scope of events through human perspectives and operational data. Such a multidimensional data structure is necessary for scientific research of war, since it combines "formal and informal" sources, providing a comprehensive basis for historical, legal, and socio-cultural analysis. In addition, military documentation plays a role in the formation of collective memory, since digital sources register not only the facts of conflict, but also become elements of a memorable narrative that transforms individual experiences into socially significant meanings. The mechanism of transformation of digital evidence into components of collective memory occurs through the re-presentation and interpretation of materials in various communication environments. Social networks, in particular, Facebook, Telegram and X are used as platforms for documenting war experiences in real time, where communities create "digital diaries" and eyewitness accounts, which are then integrated into broader narratives and discussions of events. Research has shown that Telegram has become a key platform for military communication, almost on par with conventional media, providing daily updates on air alarms, troop movements, humanitarian aid, and personal stories of civilians and fighters (Mazur, 2025). Sociological data demonstrated the widespread use of Telegram, Facebook, and YouTube as the main sources of news about the war for a significant part of the population, which turned these platforms into massive archives of human experiences and perceptions of events (Havryliuk, 2023). Specific examples illustrated how communities used hashtags and thematic categories to understand their own experiences as part of a shared story: posts tagged #war #wardiary, #війна #щоденниквійни showed regular posts about life under fire, evacuation, family relationships, and local events that not only informed, but also shaped community-wide narratives (Kot *et al.*, 2024).

These digital "war diaries" did not disappear after their initial publication, but were integrated into thematic streams, whose metadata allowed them to create chronologies, spatial maps, and thematic generalisations, which enhanced their memory function. Thus, the platform-based cyclical nature of content creation, sharing, and re-presentation contributed to the transition of individual experiences to a general social narrative, which was preserved as part of the digital cultural phenomenon of war memory. In general, digital media provided a mechanism for the constant interaction of individual and collective narratives, where personal messages were transformed into public memory texts, and content generated at the time of the event acquired post-war significance as a source of historical knowledge, ethical memory, and social identity. This process emphasised not only the role of social platforms in recording military events, but also their ability to form a shared memory through reinterpretation, thematic grouping, and integration into mass digital archives.

Empirical analysis of the corpus of digital military materials revealed a number of stable structural and semantic patterns in the practices of digital war documentation in Ukraine. The overall dynamics of the presented materials indicate a gradual transition from fragmented, decentralised forms of event recording to more ordered and standardised models of digital representation of war, combining analytical and legally oriented functions. The quantitative distribution of materials by year demonstrates an increase in institutional participation in documentation processes, especially starting in 2023. While 2022 was dominated by materials created in the form of spontaneous digital testimonies and OSINT publications, 2024-2025 was, in turn, dominated by documents with a clearly defined institutional status, formalised descriptions of events and expanded metadata support. This indicates the transformation of digital documentation from a reactive practice of crisis response to a stable element of the information and legal infrastructure of war. Analysis of the types of digital evidence showed the dominance of multimedia formats, primarily photo and video materials, which make up almost half of the sample. Their quantitative superiority is combined with high analytical and evidence-based significance, since these formats are most often used for reconstruction of events, space-time binding, and confirmation of facts in reports of human rights and international organisations. Simultaneously, a significant proportion of text documents indicate the growing role of analytical understanding and interpretation of recorded events, which complements visual data and forms integral digital narratives of war.

From the standpoint of sources of recording, the largest share is made up of materials placed in specialised digital archives that accumulate and systematise military documentation. Their dominant position indicates the gradual centralisation and institutionalisation of the digital memory of war. Official documents of state bodies and international institutions form the second largest group, performing the function of regulatory and legal framing of events. OSINT materials, although inferior in quantity, play a key role as primary sources of information that initiate further verification, archiving, and legal evaluation processes. The results of the analysis of the legal relevance of digital materials are particularly revealing. More than half of the corpus contains signs of potential suitability for use in legal proceedings, indicating a high level of documentary saturation of the digital space of war. However, a significant proportion of materials remain at the level of evidence or contextual descriptions, without being transformed into formalised evidence. This indicates that there is a gap between the mass nature of digital fixation and its full integration into legal mechanisms of prosecution. The generalised quantitative distribution of results is shown in Table 2.

Table 2. Distribution of digital military materials by key analytical parameters

Analytical parameter	**Category**	**Share (%)**
Material type	Multimedia	46.8
	Text messages	38.7
	Combined	14.5
Analytical parameter	**Category**	**Share (%)**
Source of recording	Archive platforms	41.1
	Official institutions	32.3
	OSINT environments	26.6
Legal relevance	High	58.9
	Limited	27.4
	Contextual information	13.7

Source: compiled by the authors based on a content analysis of a sample of 124 texts of digital military documentation for the period 2022-2025, including materials from archival platforms such as UWA (n.d.), official reports of the Office of the United Nations High Commissioner for Human Rights (n.d.) and U.S. Department of State (2025)

Table 2 confirms that archive platforms are gradually becoming key nodes for accumulating digital evidence, combining different types of materials, and ensuring their further interpretation and reuse. Simultaneously, the correlation between high and limited legal relevance indicates a structural tension between the volume of recorded digital evidence and the possibilities of their full legal application. This tension is a systemic characteristic of modern military conflicts, in which digital technologies significantly outstrip the pace of adaptation of legal and procedural mechanisms. As a result, the results of the empirical study show that digital documentation of the war in Ukraine has formed a multi-level ecosystem of materials, which combines eyewitness accounts, OSINT data, archival practices, and official legal documents.

The process of transforming digital evidence into collective memory narratives is connected with the fact that content created during the war does not remain passive archival material, but becomes an active participant in the memory discourse. Digital evidence is constantly circulating in the public space, re-interpreted, commented on and regrouped into thematic collections that serve as the basis for memory practices in the digital environment. The presence of such materials in the media space allows society to maintain memory in socio-political processes, forming a collective awareness of what happened and what is happening, and an identity based on the traumatic experience. Thus, digital media not only reflects events, but also plays a central role in creating memorable narratives for broad groups of society. Documentation in its nature is one of the fundamental counteractions to disinformation and historical revisionism, since military events take place simultaneously on the battlefield and in the information space (Hilmar, 2025). The social and communicative potential of military documentation is realised through the widespread use of documentary materials in the media, education, and human rights activities. Journalists and media professionals during the war use digital testimonies, photos, and videos to create full-fledged media narratives that explain the chronology of events, the scale of destruction, and the human history of the conflict. Journalists working with sensitive war content should have specific skills in evaluating, filtering, and ethically presenting digital evidence to minimise the risks of re-traumatising the audience and avoid spreading incorrect information. In turn, training programmes on media literacy and professional journalism develop skills in working with digital sources, which is necessary in the context of information warfare, where the media space simultaneously acts as an arena of information attacks and a platform for documenting real events (McDougall, 2025).

The use of military documentation in education is another dimension of the social impact of digital sources. Educational programmes include the analysis of digital evidence for the development of critical thinking in students, which allows future specialists in the humanities and social sciences to consciously interpret evidence of war, separate facts from propaganda, and evaluate the reliability of information. This approach contributes not only to professional development, but also to public maturity in understanding, documenting and preserving the memory of military conflicts. With international communication and advocacy in mind, military documentation has become a stream of information that shapes international discourses about war. Photo, video, OSINT data, and broadcasts from the scene are incorporated into reports of international organisations and human rights groups submitted to structures such as the International Criminal Court (n.d.), and are used in processes aimed at bringing to justice for war crimes. Such a mechanism confirms that digital evidence is becoming part of the justification of legal positions in international courts, where the study of civil initiatives to document war crimes in Ukraine demonstrates that the coordination of local and international efforts creates new standards of evidence for cross-border law enforcement procedures (Chlevickaitė, 2025). Thus, military documentation in the digital age is simultaneously a tool for the development of collective memory, a means of countering disinformation, a media artefact, an educational resource, and an international advocacy tool that enhances its central role in public life and the humanities.

Problems of preserving, verifying, and using digital evidence of the war in Ukraine

Digital evidence of the war in Ukraine covers a wide range of materials: photos and videos, satellite images, audio files, geolocation data, messages from smartphones and social networks, and data from drones or surveillance cameras. As of mid-2024, OSINT archive projects alone have collected millions of open-source videos. However, only a percentage of this data undergoes full-fledged expertise and analytical processing due to limited analytical resources and technological infrastructure for processing such data sets (RUSI, 2024). The collection and recording of digital evidence in military conditions is characterised by fragmentation, randomness, and unevenness. Due to the constant fighting, access to conflict zones is limited, and places of events change dynamically, which leads to missing moments, fragmented chronologies, and incomplete data. Under such conditions, digital materials are stored only on eyewitness devices or in temporary online placements, which creates the risk of loss or deletion of primary evidence. This disordered collection of data complicates their further processing and analysis, as specialists are forced to work with incomplete time or geographical labels, which reduces their evidentiary value in formal investigations. The risks of data loss are compounded by combat activities and cyber threats. In addition to direct infrastructure destruction, digital sources are subject to removal from platforms, changes in storage formats, technical obsolescence, and threats of hacker attacks. The findings of Amnesty International and its Evidence Lab indicate that large volumes of videos and photos may be "deleted or unavailable due to platform policies that respond to graphic content", making it difficult to store and capture data for a long time (Huet, 2022).

Part of the collection of digital evidence is provided by volunteer and public initiatives that create arrays of photo and video materials, coordinate geolocation and timestamps, and transmit this data to official investigative authorities. Such initiatives exceed government efforts, but their activities are highly dependent on resources and coordination, which creates uneven quality and completeness of data collected. In particular, according to Minister of Defence of Ukraine Mykhailo Fedorov, as of March 2025, the total number of reports sent by Ukrainians via the chatbot "eVorog" (Ministry of Digital Transformation of Ukraine, n.d.) during three years of full-scale war (2022-2025) exceeded 660,000, with hundreds of new reports coming in every week (Ukrinform, 2025). Establishing the origin, time, and context of the creation of digital materials is a critical step in evaluating them as evidence. Without a clear identification of the source and timestamps, digital files lose their legal significance, since the standard requirements of criminal procedure legislation regarding the admissibility of evidence provide for the establishment of a link between the facts of the event and the evidence itself. Digital data can have evidentiary value only if its authenticity is confirmed, including verification of metadata, digital signatures, timestamps and spatial binding, and strict adherence to the extraction/fixation procedure.

However, a regulatory framework in the Criminal Procedure Code of Ukraine (2012) contains gaps in the definition and procedural regulation of digital evidence. Analysis of the document shows that it does not contain clear separate provisions on "electronic (digital) evidence", and although a "document" is defined as an object containing recorded information (photos, videos, sounds, data), there is no specific procedure for collecting, recording, verifying, and evaluating digital information obtained from a network or devices. This leads to procedural difficulties and heterogeneous judicial practice when accepting digital evidence as admissible in criminal cases, in particular, when using OSINT materials, satellite images, or digital recordings (Council of Europe, 2022). The lack of a separate definition and procedure for digital evidence is one of the main barriers to their effective application in Ukrainian courts. Thus, the scale of citizens' participation in digital documentation of the war in Ukraine demonstrates the potential of digital evidence as sources of evidence, but the existing regulatory and procedural gaps in the Criminal Procedure Code of Ukraine limit their direct admissibility in criminal proceedings, which requires further legislative and expert adaptation of the legal framework.

In addition to structural barriers, digital materials are vulnerable to manipulation, deepfake technologies, and secondary editing, which creates additional difficulties in evaluating them. Artificial intelligence algorithms can create high-quality manipulated images and videos that are difficult to distinguish from authentic ones without specialised tools. This is a threat to the credibility of digital evidence in judicial and historical contexts, as it requires the development and implementation of methods that can counteract such threats (Sabin, 2025). Metadata such as timestamps, geolocation coordinates, and digital signatures is crucial in the process of verifying and authenticating digital evidence. They allow linking a digital file to a specific time and place of the event, which is necessary for establishing evidence lines in legal proceedings and historical reconstructions. In practice, international standards such as the Berkeley Protocol (recognised OSINT verification standard) are used to ensure the admissibility and reliability of digital evidence in courts and international tribunals (National School of Judges of Ukraine, 2025). Table 3 shows the main risks and methods of verifying digital evidence of war and illustrates the relationship between the main threats and practical approaches to their cybercriminalistic resolution.

Analysis of Table 3 shows that the introduction of system verification methods plays a central role in improving the reliability of digital evidence of war. A systematic combination of OSINT tools, forensic metadata

analysis, international standards, and professional training reduces the impact of fragmentation, technical limitations, and manipulation threats. Simultaneously, legal regulation and standardisation of procedures are factors that will determine whether digital evidence will be acceptable in international and national trials. In the context of the war in Ukraine, the creation of such structural and procedural decisions is necessary to create a reliable evidence base that can withstand the tests of both courtroom and historical reconstructions.

Table 3. Key risks and methods for verifying digital evidence of war

Main risks	Risk description	Verification and counteraction methods
Data fragmentation and unevenness	Data from different sources has an incomplete chronology, disparate time and geographical labels	Using OSINT tools for correlating time and geolocation tags, integrating various sources
Risks of losses due to military operations and technical restrictions	Destruction of devices, unavailability of platforms, deletion of content	Archiving on reliable digital platforms, regular backups
Manipulation, deepfake, and secondary editing	AI-generated content creates potentially fake media	Use of digital forensics, metadata analysis, spectral image analysis
Lack of a standard legal procedure	Lack of regulation of digital evidence verification in the Criminal Procedure Code of Ukraine	Implementation of international protocols, development of national standards
Insufficient expert competence	Limited number of digital forensics specialists	Professional trainings, international cooperation, creation of competence centres

Note: AI – artificial intelligence
Source: compiled by the authors based on N. Huet (2022), RUSI (2024), S. Sabin (2025), National School of Judges of Ukraine (2025), Council of Europe Office in Ukraine (n.d.)

The situation with the digitisation of the archival heritage of Ukraine in the period 2022-2025 demonstrated both significant achievements and systemic challenges. Back in 2023, Ukrainian archives created more than 21 million digital copies of documents, which allowed the country to take one of the leading places in the world in terms of digitisation rates during war (Ukraine has become..., 2024). These indicators were a signal for a large-scale mobilisation of resources aimed at protecting archival heritage and preserving national memory. Some regional initiatives showed local success in this work: for example, the State Archive of the Lviv Oblast uploaded about 500 thousand digital copies to the public in 2024, including unique historical materials, which increased the availability of local sources for scientists and the general public (The Lviv archive..., 2024).

Despite these achievements, the problem is the lack of unified digital archiving standards, which makes it difficult to combine data for long-term storage and access. The lack of standards for the unification of metadata, procedures for checking, encoding, and describing digital materials, leads to fragmentation of the information space where different archived peripheral repositories can use their own approaches to data structuring, which makes it difficult to integrate them into single repositories. This is the case for wartime materials, as their legal and historical significance may be called into question in the future if there are no guarantees to preserve the integrity and identification of data. In response to such challenges, there is a debate about the optimal relationship between centralised and decentralised models for storing digital evidence. A centralised approach provides better coordination, a single quality standard, and the ability to concentrate limited resources in high-security institutions. However, decentralised initiatives, including community and volunteer projects, allow covering a wider field of real-time materials that cannot always be quickly transferred to centralised archives due to physical or technical limitations. Both approaches have their advantages and disadvantages, and their synchronisation and integration into a single archive and information ecosystem is the subject of ongoing discussions and cooperation projects.

The effective operation of the digital military evidence archiving system at the standard level depends on coordinated actions not only of technological solutions, but also of a wide range of institutional actors involved in the process: from state archives and museum institutions to media, human rights, and public organisations. These institutions implement a set of functions – they guarantee access, authenticity, and data protection and create the basis for their scientific, legal, and memorable use. State archives in Ukraine play a role in shaping digital data storage strategies. As part of digitisation projects, platforms such as the Interarchive Search Portal (State Archival Service of Ukraine, n.d.), where, as of 1 January 2025, more than 2.5 million digital copies of documents from the National Archival Fund have been made public, expanding access for researchers and the public to archival heritage materials in digital form. Museum and library institutions, such as Dovzhenko Centre (n.d.), actively digitise audiovisual and cultural artefacts of historical and documentary value during the war, creating digital collections available for further analysis.

The legal and ethical aspects of the use of digital military documentation appear as the basic conditions for its sustainable preservation and further application in scientific, legal, and memorial contexts. The central

issue in this dimension remains the protection of personal data and the security of witnesses, as digital archives accumulate sensitive information about individuals, including data on the locations of participants in the conflict, contact information, and personal eyewitness accounts. Analysis of the practices of Ukrainian archives shows that the mechanisms for regulating access to materials with personal data remain institutionally incomplete, which significantly limits the possibility of their public use without the presence of developed legal and ethical control tools. In this context, the principles of confidentiality, minimisation of processing, and proportionality of access to data, the level of which should correspond to the risks for persons whose data are stored, appear as fundamental regulatory guidelines for the implementation of digital archival practices at the national and international levels (Parmelee *et al.*, 2025).

The results obtained are organically integrated into the contemporary scientific discourse, while expanding it through a comprehensive understanding of digital military documentation as a multidimensional phenomenon that combines legal evidence, archival value, and the functions of a collective memory carrier. The study showed that the effectiveness of digital documentation of war is determined not so much by technical or institutional solutions, but by the ability to integrate legal, archival, and socio-cultural approaches into a single sustainable system focused on long-term memory preservation, ensuring justice, and maintaining cultural identity. In this sense, the results are conceptually correlated with the findings of O. Hudoshnyk *et al.* (2025), who interpreted the massive mediatisation of military experience through participating initiatives and digital archives as a factor in transforming the memory landscape, where user-generated content acquires the status of an element of historical narrative. The current study expands this opinion, demonstrating that digital evidence functions not only in the media and therapeutic dimensions, but also forms the evidence base and objects of long-term archival storage, which creates tension between the emotional, memorial, and procedural and legal logic of their use.

Analysis of the problem of remote documentation of war crimes revealed a conceptual relationship with the provisions of P.R. Williams & N. Carle (2023), who saw remote documentation as an innovative response to limited physical access to war zones, emphasising the importance of digital infrastructure, cybersecurity, and ethical online interaction protocols. The results confirmed the effectiveness of this approach in the context of the Ukrainian conflict, but simultaneously showed its structural limitations: the collected data sets are often characterised by incomplete metadata, which complicates their legal verification and integration into national judicial procedures. Thus, remote documentation appears as an effective tool for initial collection, which, however, requires institutional refinement to transform into procedurally valid evidence. The results of the study also correlate with the findings of Y. Kovalenko (2025) regarding the role of digital archives in maintaining the historical memory and cultural identity of Ukraine. The importance of audiovisual archives as sources of humanistic knowledge and global communication is confirmed, but the data obtained raises questions about the excessive fragmentation of archival initiatives. In contrast to the emphasis on the positive potential of decentralised practices, the study showed that the lack of unified metadata standards and coordination mechanisms creates risks of loss of context and reduced analytical value of materials in the long term. A. Koenig's (2022) opinion on the paradigm shift from centralised models of evidence gathering to decentralised and collaborative forms is also within this conceptual field. These ideas are consistent with the conclusions about the transformation of military documentation into a complex semiotic complex formed at the intersection of state, public, and individual practices. Simultaneously, the study complemented the legal interpretation of digital evidence with a socio-cultural dimension, demonstrating their role in the documentation of collective memory and memorial narratives.

The concept of a standardised digital infrastructure for documenting war crimes, proposed by I. Svoboda *et al.* (2025), also found confirmation in the results of a study that identified a critical shortage of unified archiving standards, metadata descriptions, and digital evidence verification procedures. The hybrid model proposed by the researchers conceptually corresponds to the recorded trend towards interdisciplinary convergence of technological, legal, and ethical approaches. The results of the study detailed the limitations of this approach, in particular, data fragmentation, uneven geographical coverage, and dependence on digital platform policies that directly affect the long-term preservation of evidence arrays. Analytical observations by M. Makhortykh (2023) on the vulnerabilities of digital platforms as military evidence storage environments are in direct line with the identified risks of losing primary materials due to technical failures, infrastructure destruction, and enterprise solutions of private platforms. The study expanded this approach, demonstrating that fragmentation or loss of digital materials affects not only historical reconstruction, but also the legal admissibility of evidence and the processes of collective memory documentation, which actualises the need for synergy between state archives, museums, public initiatives, and international institutions, while simultaneously consolidating these practices. A similar logic can be traced in relation to the provisions of L.L.R. Roush (2023), who emphasised the lack of effective preventive international mechanisms for documenting cultural heritage during armed conflicts. In line with the conclusions about the fragmentary nature of digital evidence collection, the study further emphasised the semiotic and sociocultural dimensions of digital documentation, in particular, its ability to form long-term narratives

of collective memory and maintain cultural identity in the digital environment, which goes beyond the purely judicial and reparatory interpretation.

Thus, the technological, legal, and ethical components of archiving digital military evidence form an interdependent system, the development of which is impossible within the framework of isolated approaches. Large-scale implementation of innovative technologies should be accompanied by unification of standards, inter-institutional coordination, integration with international norms, and clear regulation of the protection of human rights, in particular, the privacy and security of witnesses. It is this integrated approach that creates the grounds for transforming digital military documentation into a legally acceptable, scientifically valid, and socially significant resource of the collective memory of society.

Conclusions

In the course of the study, it was found that military documentation in the digital age was transformed into a complex semiotic complex, which found itself at the intersection of historiography, archival studies, memorial studies, digital humanities, and jurisprudence, forming new approaches to recording, interpreting, and preserving traces of conflict. The deployment of a full-scale war in Ukraine since 2022 has been a catalyst for the emergence of one of the world's largest digital evidence arrays, including millions of multimedia files, OSINT materials, official documents, and eyewitness accounts that have acquired both historical, legal, and socio-cultural value. It was demonstrated that these digital artefacts not only passively recorded events, but also actively participated in the processes of collective memory documentation, transforming individual experiences into socially significant narratives through mechanisms of circulation in social networks and digital archives. The classification of types of digital military documentation revealed their functional complementarity: official government documents provided legal and administrative legitimation of facts; centralised digital archives and databases, such as the Ukraine War Archive, provided system storage and structuring of metadata; multimedia materials formed a visual chronology and became a tool for forensic reconstruction; while eyewitness accounts and OSINT sources expanded the contextual understanding of the conflict, introducing the human dimension and operational data into the documentation, which turned out to be necessary for social memory research.

Simultaneously, systemic problems were identified that accompanied the documentation process. The collection of digital evidence in the context of active combat operations has proved fragmented and uneven, resulting in data sets with incomplete time and geographical labels, while technical limitations, infrastructure destruction, digital platform policies, and cyber threats have created high risks of losing primary materials. The critical challenge was the insufficient regulatory framework: the analysis of the Criminal Procedure Code of Ukraine showed the lack of a clear definition and special procedural regulation for digital (electronic) evidence, which led to heterogeneity of judicial practice and limited their direct admissibility in national criminal proceedings. In addition, the proliferation of deepfake technologies and secondary editing capabilities have jeopardised trust in the authenticity of digital materials, requiring the development of sophisticated verification techniques such as metadata analysis, spectral image analysis, and the introduction of international protocols such as the Berkeley Protocol. The large-scale mobilisation of public resources allowed achieving success in digitisation, which laid the material foundation for long-term memory preservation, but the lack of unified archiving standards and metadata created risks of fragmentation of the information ecosystem.

The social and communicative potential of military documentation was implemented through its active use in the media, education, and international advocacy. Journalists, human rights defenders, and educators have turned digital evidence into tools for forming public narratives, developing critical thinking, and building an evidence base for international courts, including the International Criminal Court. Synergy between state archives, museums, public initiatives, and international institutions proved necessary for the development of a sustainable multidimensional system capable of ensuring the legal admissibility, scientific validity, and socio-cultural significance of digital military documentation. A limitation of the study was the lack of regulatory and standardised procedures for verifying digital evidence in national legislation, which makes it difficult to use them directly in criminal proceedings. The prospects are to develop common archival and information standards and interdisciplinary methodologies that combine legal, technological, and ethical approaches to transform digital arrays into a long-term tool for justice, science, and collective memory documentation.

Acknowledgements

None.

Funding

None.

Conflict of Interest

None.

References

[1] Bareikytė, M., & Makhortykh, M. (2024). Digitally witnessable war from pereklychka to propaganda: Unfolding Telegram communication during Russia's war in Ukraine. *Media, War & Conflict*, 18(3). doi: 10.1177/17506352241255890.

[2] Bonjack, S. (2025). Preserving cultural heritage in times of war. *Performing Arts Resources*, 37, article number 8. doi: 10.3998/par.7445.
[3] Chlevickaitė, G. (2025). Documenting conflict-related crimes in Ukraine: Civil society innovations, adaptations and networks in the accountability ecosystem. *Journal of International Criminal Justice*, 23(3-4), 523-543. doi: 10.1093/jicj/mqaf020.
[4] Christensen, B., & Khalil, A. (2023). Reporting conflict from afar: Journalists, social media, communication technologies, and war. *Journalism Practice*, 17(2), 300-318. doi: 10.1080/17512786.2021.1908839.
[5] Council of Europe Office in Ukraine. (n.d.). *CyberUA: Strengthening capacities on electronic evidence of war crimes and gross human rights violations in Ukraine*. Retrieved from https://www.coe.int/en/web/kyiv/cyberua.
[6] Council of Europe. (2022). *Country profile: Ukraine – Budapest Convention on Cybercrime*. Retrieved from https://www.coe.int/en/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/ukraine/pop_up.
[7] Criminal Procedure Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17?lang=en#Text.
[8] da Costa, A.A., & Santos, L.R.M. (2023). Polycam and the power of heritage registration in the palm of your hand: UNESCO strategy to safeguard memory in Ukraine war. In R. Christofoletti (Ed.), *Soft power and heritage* (pp. 67-81). Cham: Springer. doi: 10.1007/978-3-031-41207-3_4.
[9] Dovzhenko Centre. (n.d.). Retrieved from https://dovzhenkocentre.org/en/.
[10] Ellis, M.S. (2025). Investigating and documenting war crimes in Ukraine. In Y. Dutton, M.P. Scharf, M. Sterio & P.R. Williams (Eds.), *Ukraine and the legal accountability of Russia: The emergence of a new global order* (1st ed., pp. 189-214). London: Routledge. doi: 10.4324/9781003458166-14.
[11] Gentile, M. (2025). War memorialization and nation-building in Ukraine. *Eurasian Geography and Economics*, 66(7), 765-792. doi: 10.1080/15387216.2025.2498159.
[12] Havryliuk, O. (2023). Statistics and trends in the functioning of social networks. *Digital Platform Information Technologies in Sociocultural Sphere*, 6(2), 383-397. doi: 10.31866/2617-796X.6.2.2023.293609.
[13] Hilmar, T. (2025). Signifying the present in links to the past: Memory organizations react to the February 24, 2022, Russian full-scale invasion of Ukraine. *American Journal of Cultural Sociology*. doi: 10.1057/s41290-025-00267-7.
[14] Hoskins, A., & Shchelin, P. (2023). The war feed: Digital war in plain sight. *American Behavioral Scientist*, 67(3), 449-463. doi: 10.1177/00027642221144848.
[15] Hudoshnyk, O., Krupskyi, O.-P., & Styrnik, N. (2025). Mediatization of collective testimonies during the Russian-Ukrainian War 2022-2023. *Communication & Society*, 38(1), 281-297. doi: 10.15581/003.38.1.021.
[16] Huet, N. (2022). *How digital evidence of war crimes in Ukraine is being collected, verified and preserved*. Retrieved from https://www.euronews.com/next/2022/04/06/how-digital-evidence-of-war-crimes-in-ukraine-is-being-collected-verified-and-stored.
[17] International Criminal Court. (n.d.). Retrieved from https://www.icc-cpi.int/.
[18] Judiciary of Ukraine. (2025). *OSINT as evidence in the investigation of war crimes: Representatives of the Supreme Court participated in a thematic seminar*. Retrieved from https://court.gov.ua/press/news/1883704/.
[19] Khan, S.A., Furuly, J.G., Vold, H.B., Tahseen, R., & Dang-Nguyen, D.-T. (2023). Online multimedia verification with computational tools and OSINT: Russia-Ukraine conflict case studies. *arXiv*. doi: 10.48550/arXiv.2310.01978.
[20] Koenig, A. (2022). From 'Capture to Courtroom': Collaboration and the digital documentation of international crimes in Ukraine. *Journal of International Criminal Justice*, 20(4), 829-842. doi: 10.1093/jicj/mqac046.
[21] Kot, S., Mozolevska, A., & Polishchuk, O. (2024). Digital war diaries: Witnessing the 2022 Russian war against Ukraine. *Memory, Mind & Media*, 3, article number e15. doi: 10.1017/mem.2024.11.
[22] Kovalenko, Y. (2025). Digital preservation of Ukrainian audiovisual heritage during wartime: Challenges and institutional practices. *Culture Crossroads*, 27, 200-212. doi: 10.55877/cc.vol27.534.
[23] Lytvynska, S.V. (2014). And once again about documentology. *Library Science. Record Studies. Informology*, 1, 47-52.
[24] Makhortykh, M. (2023). Unreliable narrators or untimely archivists? Challenges of using digital platforms for documenting and remembering Russia's war in Ukraine. *Georgetown Journal of International Affairs*, 24(2), 165-173. doi: 10.1353/gia.2023.a913642.
[25] Mandolessi, S. (2024). Memory in the digital age. *Open Research Europe*, 3, article number 123. doi: 10.12688/openreseurope.16228.2.
[26] Mazur, D.V. (2025). *The role of the media in the Russian-Ukrainian war*. (Master's thesis, Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine).
[27] McDougall, J. (2025). What do we think about when we talk about media literacy? In *Media literacy for the communication ecosystem: A theory of change for a healthier future* (pp. 77-150). Cham: Springer. doi: 10.1007/978-3-032-04024-4_4.

[28] Meta Platforms, Inc. (n.d.). *Facebook*. Retrieved from https://www.facebook.com/.
[29] Ministry of Digital Transformation of Ukraine. (2024). *The digital archive of documents about the Russian-Ukrainian war has collected over 4,000 documents from different regions of Ukraine*. Retrieved from https://mincult.gov.ua/news/czyfrovyj-arhiv-dokumentiv-pro-rosijsko-ukrayinsku-vijnu-zibrav-ponad-4000-dokumentiv-z-riznyh-regioniv-ukrayiny/.
[30] Ministry of Digital Transformation of Ukraine. (n.d.). *eVorog (Chatbot)*. Retrieved from https://evorog.gov.ua/.
[31] National School of Judges of Ukraine. (2025). *Digital trace as evidence: New standards of judicial evaluation*. Retrieved from https://nsj.gov.ua/ua/news/tsifroviy-slid-yak-dokaz-novi-standarti-sudovogo-otsinuvannya/.
[32] Ochi, M., & Dagenborg, H. (2025). Online war-crime archives: A call for a universal guideline. In A. Galushko & M. Ochi (Eds.), *Collecting cyber evidence during ongoing hybrid warfare* (Chapter 8). Antwerp: Maklu-Garant. doi: 10.2139/ssrn.5128953.
[33] Office of the United Nations High Commissioner for Human Rights. (n.d.). *Reports*. Retrieved from https://ukraine.ohchr.org/en/reports.
[34] Oxendine, C. (2022). *Ukraine: Open-source data aided response and documents damages and atrocities*. Retrieved from https://www.esri.com/about/newsroom/blog/ukraine-open-source-intelligence.
[35] Parmelee, J.H., Roman, N., & Beasley, B. (2025). Moral framing in Ukraine war coverage. *Media, War & Conflict*, 18(3), 366-382. doi: 10.1177/17506352241264197.
[36] Pédauque, R.T. (2022). Document: Form, sign, and medium, as reformulated by digitization. In G. Hartung, F. Schlupkothen & K.-H. Schmidt (Eds.), *Using documents: A multidisciplinary approach to document theory* (pp. 225-260). Berlin, Boston: De Gruyter. doi: 10.1515/9783110780888-009.
[37] Ragni, C. (2023). Digital evidence in international criminal proceedings and human rights challenges. *EU and Comparative Law Issues and Challenges Series (ECLIC)*, 7, 1183-1202. doi: 10.25234/eclic/28255.
[38] Roush, L.L.R. (2023). *Heritage under threat: Documentation methods for preserving at-risk cultural identity and prosecuting cultural heritage war crimes during the Russo-Ukrainian war*. (Master's thesis, Johns Hopkins University, Baltimore, United States).
[39] Royal United Services Institute (RUSI). (2024). *Puzzling pieces: OSINT and war crime accountability in Ukraine*. Retrieved from https://www.wired-gov.net/wg/news.nsf/articles/Puzzling%2BPieces%2BOSINT%2Band%2BWar%2BCrime%2BAccountability%2Bin%2BUkraine%2B30092024092500.
[40] Sabin, S. (2025). *Courts aren't ready for AI-generated evidence*. Retrieved from https://www.axios.com/2025/07/25/courts-deepfakes-ai-trial-evidence.
[41] State Archival Service of Ukraine. (n.d.). *Interarchive Search Portal*. Retrieved from https://searcharchives.net.ua/.
[42] Svoboda, I., Husak, A., Koller, Y., Kosytsia, O., & Karasov, V. (2025). Digital technologies in documenting war crimes: Legal and ethical aspects. *Journal of Theoretical and Applied Information Technology*, 103(20), 8393-8410.
[43] Telegram Messenger LLP. (n.d.). Retrieved from https://t.me/telegram.
[44] The Lviv archive has uploaded half a million copies of unique historical documents to the internet. (2024). Retrieved from https://odessa-journal.com/the-lviv-archive-has-uploaded-half-a-million-copies-of-unique-historical-documents-to-the-internet.
[45] U.S. Department of State. (2025). *2024 country reports on human rights practices: Ukraine*. Retrieved from https://www.state.gov/reports/2024-country-reports-on-human-rights-practices/ukraine.
[46] Ukraine has become the second country in the world in terms of the scale of document digitization. (2024). Retrieved from https://odessa-journal.com/public/index.php/ukraine-has-become-the-second-country-in-the-world-in-terms-of-the-scale-of-document-digitization.
[47] Ukraine War Archive (UWA). (n.d.). Retrieved from https://ukrainewararchive.org/eng/.
[48] Ukrinform. (2025). *Ukrainians send hundreds of messages every week through the "eVorog" chatbot – Fedorov*. Retrieved from https://www.ukrinform.ua/rubric-society/3973950-cerez-catbot-evorog-ukrainci-nadsilaut-sotni-povidomlen-sotizna-fedorov.html.
[49] Vonnák, D., Jones, S., Rasmussen, J., & Hardy, S. (2025). *Mobilising care for cultural heritage in Russia's war against Ukraine*. Stirling: University of Stirling. doi: 10.34722/n9m2-tv84.
[50] Williams, P.R., & Carle, N. (2023). The war in Ukraine: A case study in modern atrocity crimes documentation. *Case Western Reserve Journal of International Law*, 55(1), 7-40.
[51] X Corp. (n.d.). Retrieved from https://x.com/.

Воєнна документація як джерело історичної пам'яті: проблеми збереження цифрових доказів війни в Україні

Алла Зленко
Кандидат історичних наук, професор
Університет Григорія Сковороди в Переяславі
08401, вул. Сухомлинського, 30, м. Переяслав, Україна
https://orcid.org/0000-0002-5586-3984
Юрій Лященко
Викладач
Університет Григорія Сковороди в Переяславі
08401, вул. Сухомлинського, 30, м. Переяслав, Україна
https://orcid.org/0009-0007-1302-6823
Надія Різник
Викладач
Університет Григорія Сковороди в Переяславі
08401, вул. Сухомлинського, 30, м. Переяслав, Україна
https://orcid.org/0000-0003-0893-9795

Анотація. Метою статті було проаналізувати роль воєнної документації у конструюванні історичної та соціальної пам'яті та дослідити специфічні виклики, пов'язані зі збереженням цифрових свідчень війни в Україні. У роботі було застосовано комплексний міждисциплінарний підхід, який через нормативно-правовий, документознавчий, порівняльний та контент-аналіз охопив законодавчі акти, інституційні практики, архівні проєкти, цифрові платформи та матеріали відкритих джерел, що забезпечило змогу простежити механізми створення, збереження, верифікації та використання цифрових доказів війни. У ході дослідження було встановлено, що цифрова воєнна документація трансформувалася з допоміжного інформаційного ресурсу в центральний елемент фіксації війни, набувши одночасно доказового, меморіального та комунікативного значення. Проаналізовано, що повномасштабна війна зумовила формування одного з найбільших у світі масивів цифрових доказів, який включає офіційні документи, мультимедійні матеріали, супутникові знімки та свідчення очевидців. Було виявлено функціональну взаємодоповнюваність різних видів цифрової документації, де державні архіви забезпечували правову легітимацію, а громадські та медійні ініціативи – оперативність і соціальну репрезентацію подій. Аналіз нормативної бази показав наявність прогалин у процедурному регулюванні статусу цифрових доказів, що призводить до неоднорідності правозастосовної практики. Дослідження інституційних практик засвідчило прогрес у масштабах оцифрування архівних фондів, водночас виявивши проблему фрагментації стандартів зберігання та метаданих. Окремо було доведено, що поширення технологій маніпуляції цифровим контентом актуалізувало потребу у впровадженні складних процедур верифікації та міжнародних протоколів оцінки доказів. Зроблено висновок, що ефективне збереження та використання цифрової воєнної документації можливе лише за умов координації державних, громадських і міжнародних інституцій на основі уніфікованих правових, технічних та етичних стандартів. Результати дослідження орієнтовані на архівістів, правників, дослідників гуманітарного профілю, журналістів і фахівців з документування воєнних злочинів, які працюють із цифровими доказами війни та формуванням історичної і колективної пам'яті

Ключові слова: архіви; мультимедійні матеріали; свідчення очевидців; дезінформація; злочини