Journal of Theoretical and Applied Information Technology
31st October 2025. Vol.103. No.20

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

DIGITAL TECHNOLOGIES IN DOCUMENTING WAR CRIMES: LEGAL AND ETHICAL ASPECTS

IVO SVOBODA[1] , ANDRII HUSAK [2], YURII KOLLER[3], OLHA KOSYTSIA[4], VALENTYN KARASOV[5]

[1]Associate Professor, Guarantor of Security Management Studies, AMBIS, a.s. Vyská škola, Prague, Czech Republic

[2]Doctor of Law, Lesya Ukrainka Volyn National University, Department of Criminal Law and Procedure, Lutsk, Ukraine

[3]PhD in Law, Senior Research Fellow, Research Laboratory on State-Building and Law Enforcement Problems of the Educational and Scientific Institute of Law and Psychology of the National Academy of Internal Affairs, Kyiv, Ukraine

[4]Doctor of Law, Professor, Interregional Academy of Personnel Management, Department of Law Enforcement and Anti-Corruption Activities of the Educational and Scientific Institute of Law named after Volodymyr Velykyi, Kyiv, Ukraine

[5]Postgraduate student, Higher Educational Institution "University of Economics and Law 'KROK'", Kyiv, Ukraine

E-mail: [1]svobodaivo985@gmail.com, [2]andriihusak123@gmail.com, [3]yuriikoller48@gmail.com, [4]okosytsia@gmail.com, [5]valentynkaras256@gmail.com

ABSTRACT

The relevance of the research

The relevance of the research is determined by the need to create a standardized, legally verified, and ethically acceptable digital infrastructure for documenting war crimes in the context of growing volumes of digital evidence, interjurisdictional fragmentation, and the needs of post-conflict society in mechanisms for reparations and ensuring human rights.

Aim of the research

The aim of the research is to formalize and model the framework of a global digital platform for documenting war crimes, taking into account multi-source aggregation, forensic validation, legal stratification, and institutional interoperability in accordance with international standards.

Methods of the research

The research methodology consists of: comparative analysis of digital technologies, synthetized framework modelling, ontological modelling, functional and procedural modelling, scenario sequence modelling.

Obtained results

A comparative analysis of digital technologies for documenting war crimes revealed differentiation of evidentiary capacity according to the parameters of chain of custody, forensic reliability, metadata control, and normative congruence, which is critically important in the context of protecting human rights and implementing procedures for compensation for damage caused by military actions. Digital repositories and mobile evidence applications demonstrated the highest evidentiary stability, while artificial intelligence (AI)/machine learning (ML) modules and automated attribution systems have risks of bias, opacity of inference, and limited explainability. In response to the identified challenges, a hybrid framework was developed with a synthesis of Open Source Intelligence (OSINT), Geospatial Intelligence (GEOINT), blockchain, AI/ML, which ensures traceological integrity, legal validity and cross-jurisdictional interoperability of digital evidence in the context of post-conflict justice. The framework for digital documentation of war crimes is focused not only on optimizing the evidentiary process, but also on integration into mechanisms for protecting human rights and transitional justice.

Academic novelty of the research

The academic novelty of the research is the formalization of an integrated forensic legal framework of a digital platform for documenting jus in bello crimes, which combines AI/ML discrimination, blockchain anchoring, OSINT/GEOINT aggregation, metadata control, and legal stratification. The article is the first to

develop an ontology of inter-component interaction focused on preserving chain of custody, tamper-resistance, explainability, and transjurisdictional admissibility.

Prospects for further research

Further research may focus on the development of a pilot project with phased validation of the framework in simulated criminal proceedings. The testing should cover the criteria of procedural relevance, evidentiary integrity, and transjurisdictional consistency.

Keywords: *Human Rights, Reparation Of Damages, Reparation For War-Related Damages, Post-Conflict Society, Transitional Justice, Digital Platform, Evidentiary Framework*

1. INTRODUCTION

The escalation of armed conflicts and the increasing number of crimes against humanity has made the issue of proper recording, verification, and presentation of digital evidence a priority in the context of international criminal justice, transitional justice, and human rights protection. Digital technologies — in particular OSINT, GEOINT, AI/ML systems, blockchain records, and mobile witness applications — are actively integrated into human rights protection and monitoring mechanisms. At the same time, they remain normatively unharmonized, fragmentedly applied, and limited in evidentiary admissibility, in particular with regard to issues of compensation for damage caused by military operations.

The necessity of this study is substantiated by the lack of a unified, legally stratified and procedurally resilient digital framework for the fixation of jus in bello violations under conditions of high evidentiary fragmentation, limited metadata verifiability, and interjurisdictional incongruence. The research addresses this gap through the formalisation of a hybrid forensic-legal architecture that ensures compliance with chain of custody, tamper-resistance, explainability, and admissibility, thereby enhancing the infrastructural capacity for digital accountability in contexts of transitional justice and post-conflict societal reconstruction.

The lack of a coherent interoperable infrastructure complicates procedural traceability, authentication of digital artifacts and transjurisdictional recognition of materials in international courts (International Criminal Court (ICC), European Court of Human Rights (ECHR), United Nations (UN) Fact-Finding Mechanisms), especially in the context of post-conflict society. Existing approaches are typically descriptive or operationally isolated, and do not provide system integration of components taking into account the principles of chain of custody, due process, privacy-by-design, and metadata verifiability.

The aim of the research is to develop, structurally formalize, and verify the framework of a global digital platform for recording war crimes, combining multi-source aggregation, forensic validation, legal stratification and institutional interoperability in accordance with the standards of international humanitarian and criminal law.

Research objectives:

1. Carry out a comparative analysis of digital technologies for recording war crimes according to the criteria of legal and ethical admissibility;
2. Form a synthesis concept of the architecture of a global digital evidentiary platform;
3. Develop an ontological model of the semantic relationships of the platform components.
4. Perform functional and procedural modelling of data processing and verification procedures.
5. Model the scenario sequence interaction of digital components within the evidentiary cycle.

2. LITERATURE REVIEW

The evolution of digital means of recording violations of international humanitarian law (IHL) necessitates the analysis of academic approaches to their evidentiary relevance, procedural admissibility, as well as ethical and legal admissibility. This section covers relevant academic concepts that shape the modern understanding of the digital evidentiary ecosystem, its normative stratification, and forensic integration into the structure of international criminal prosecution.

In particular, the author [1] classified visual journalism of war as a component of the digital evidentiary ecosystem that provides indexing of facts of IHL violations through photo and video data. The paper identifies regulatory and mediating imperatives that determine the boundaries of ethical and legal admissibility, procedural authenticity, and forensic validity of digital evidence.

Similarly, the authors [2] introduce the concept of affective epistemology as a factor in the cognitive legitimation of digital journalistic evidence in the documentation of war crimes. The emotional involvement of media professionals is interpreted as a methodological tool and epistemic resource that increases evidentiary relevance and consistency with the principles of legal fact-finding.

Another aspect was revealed by [3], who investigated the procedural admissibility and probative value of digital evidence in the criminal process of the ICC (art. 69(4)). A shift towards the forensic validity of video and satellite materials Under the influence of civilian evidentiary activity in the context of the armed conflict in Ukraine was recorded.

Accordingly, the author [4] established the epistemological weight of digital testimony and evidence in the structure of the ICC forensic process, focusing on their impact on verdict validity. The study substantiates the critical role of procedural controllability of witnesses and evidentiary rigour as key conditions for ensuring legal accountability for war crimes.

The authors [5] studied the technical aspects and classified 52 online war crimes archives as evidentiary, normative, and memorial repositories. The authors argued for the need for standardized secure archiving protocols that guarantee legitimacy, informational integrity, and ethical non-harm in transitional justice processes.

The researcher [6] explored the ethical aspect and analysed the visual representation of death in armed conflicts through the prism of IHL, international human rights law (,) and international criminal law (ICL), focusing on the legitimacy and ethical admissibility of publishing images of the dead. The author argued for the need for revising the regulatory landscape, taking into account digital permanence, asymmetric visualization of violence, and deontological protection of post-mortem dignity.

The author [7] identified another technical and procedural aspect, who analysed the evidentiary risks of digital content in military legal proceedings, in particular, chain of custody violations, AI modification, and disinformation campaigns. The authors [8] emphasized the need for institutionalized mechanisms for verification, archiving and procedural admissibility of digital evidence in the practice of international criminal responsibility.

The authors [9] found the regulatory issue, who investigated the collision between information access and digital privacy within OSINT investigations into violations of IHL, ICL, and IHRL. The need for universalization of evidentiary standards, including admissibility, attribution, chain of custody, and meta-information validation in accordance with the Berkeley Protocol, is substantiated to ensure transnational procedural legitimacy in the investigations, including war crimes.

The researchers [10] covered similar issues, who analysed the forensic and procedural aspects of digital evidence of war crimes in the Russian-Ukrainian war in the victim-centric transitive justice. The authors [11] emphasized the need for unification of attribution protocols, admissibility of OSINT evidence, and regulatory adaptation of digital recording methods to the requirements of international criminal jurisprudence.

Finally, the author [12] substantiated the need for a doctrinal revision of the evidentiary paradigm in connection with the massive digital accumulation of evidence of war crimes in Ukraine, in particular through online questionnaires, OSD databases, and video evidence. The author emphasized the need to implement algorithmic triage mechanisms, metadata auditing, standardized forensic validation protocols, and machine-guided digital chain of custody management.

The analysis of the corpus of publications has shown the emergence of a new digital evidentiary paradigm, in which war crimes are documented through OSINT sources, algorithmic triage, metadata audit, forensic attribution and procedural admissibility in transnational criminal proceedings. Critical discrepancies were identified in the areas of information access vs. digital privacy, evidentiary validation of visual content, chain of custody, and regulatory harmonisation of digital recording protocols in the system of international justice.

In this context, the need for a comprehensive study of digital technologies in documenting war crimes from the perspective of legal and procedural compatibility, normative universalisation, ethical and deontological admissibility, postmortem protection of dignity, as well as institutional integration of technical and forensic solutions into the structure of international criminal law and transitional justice is substantiated.

3. METHODS AND MATERIALS

3.1. Research design

Figure 1 graphically presents the research iterations.

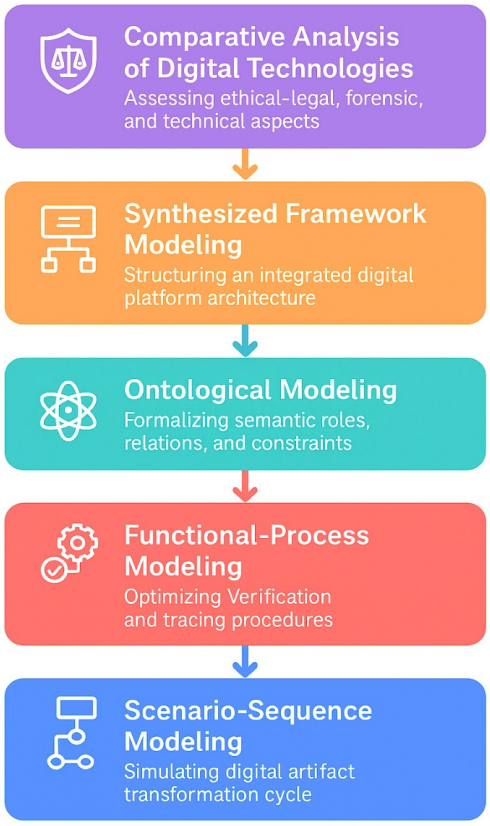

Figure 1: Research design

Source: created by the authors

3.2. Methods

The study applied five complementary methods:

1. *Comparative analysis of digital technologies for documenting war crimes* was applied for a multidimensional assessment of digital solutions according to the criteria of ethical and legal admissibility, forensic reliability, technical interoperability, and compliance with international standards (ICC, ECHR, UN).

2. *Synthetised framework modelling of the global digital platform for documenting war crimes* provided the architectural structuring of an integrated system that combines OSINT, GEOINT, AI/ML, blockchain, and digital repositories into a single evidentiary infrastructure in compliance with the principles of chain of custody and due process.

3. *Ontological modelling of the framework of the global digital platform for documenting war crimes* formalized the semantic roles of components, the logic of their relationships, regulatory constraints, and procedural trajectories within the digital evidence ecosystem.

4. *Functional and procedural modelling of the framework of the global digital platform for documenting war crimes* aimed at optimizing the procedures for verifying and preserving data authenticity, tracing information flows, and ensuring regulatory compliance in the UML architecture format.

5. *Scenario sequence modelling of the framework of the global digital platform for documenting war crimes* enabled recreating the full cycle of digital artifact transformation: from multi-source collection to legally relevant presentation, identifying critical risk points and ensuring compliance with the principles of digital evidentiality.

3.3. Sample

The study included a targeted sampling of key digital technologies used to record war crimes, taking into account their functional purpose, legal and procedural status, precedents of practical use and compliance with ICC, UN, and ECHR standards — Table 1.

Table 1: Digital technologies used to record war crimes

Technology	Brief description	Implementation examples	Application precedents	Compliance with ICC / UN / ECHR standards	Academic research
OSINT-platforms (Open Source Intelligence)	Mechanisms for aggregation, structured extraction and semantic analysis of digital artifacts from open sources.	Bellingcat, Mnemonic, Truth Hounds	Syria, 2017: Bellingcat applied geospatial attribution, photogrammetry, and chronological reconstruction of video evidence of the chemical attack in Khan Sheikhoun — the materials were incorporated in the Organisation for the Prohibition of Chemical Weapon (OPCW) –UN report. Ukraine, 2022: Mnemonic performed structured fact-finding based on the video of the exhumations in Bucha —	ICC: partial evidentiary admissibility under Art. 69(4); UN: application in the International, Impartial and Independent Mechanism (IIIM) (Syria), Fact-Finding Mission (FFM) (Myanmar); ECHR: not recognized as autonomous evidence, but can be used in the	Dodds et al. [13]; Flamer [14]

Technology	Brief description	Implementation examples	Application precedents	Compliance with ICC / UN / ECHR standards	Academic research
			the materials were transferred to the Prosecutor General's Office (PGO) and incorporated into the preliminary evidentiary matrix of the ICC.	context of supporting evidence.	
Geospatial intelligence (GEOINT)	Remote Sensing Instruments (RSI) using multispectral imaging to document the spatial consequences of attacks	Maxar, Planet Labs, UNOSAT	Darfur, 2009: Maxar provided infrared spectral imaging of ethnic cleansing areas, which became part of the UN intelligence analysis for the case against al-Bashir (ICC). Ukraine, 2022: Maxar satellite imagery was used to forensically localize the destruction of a maternity hospital in Mariupol — entered into the Office of the UN High Commissioner for Human Rights (OHCHR) registry.	ICC: admissibility taking into account chain of custody and independent verification; UN: fully compliant with OHCHR/ United Nations Satellite Centre (UNOSAT) standards; ECHR: admissible in cases under Articles 2, 3 and 8 (right to life, prohibition of torture, privacy).	Riefda Novikarany [15]; Dickey & Gleason [16]
Digital evidence repositories	Repositories with metadata indexing, hash function, and chain of custody support.	eyeWitness, Bayanat Box	The Central African Republic (CAR), 2016–2019: eyeWitness collected digital evidence of Anti-Balaka crimes with automated generation of the evidence transmission chain — the materials were incorporated into the indictment in the Ngaïssona Case (ICC). Ukraine, 2022: repositories recorded the signature integrity (SHA-256) of media files transferred to the PGO cooperation section with Eurojust.	ICC: high compliance with chain of custody requirements; UN: supported by ehe United Nations Human Rights Council (UNHRC), the Investigative Team to Promote Accountability for Crimes Committed by Da'esh/ISIL (UNITAD); ECHR: considered relevant subject to procedural due process requirements.	Rose [17]; Florczak, Jach & Rosłon-Żmuda [18]
AI/ML verification systems	Algorithms for classifying the incoming stream of digital data, detecting semantic inversion, video manipulations, and synthetic artifacts.	Truepic, Hala Systems	Yemen, 2020: Hala Systems identified vector artifacts of algorithmic compression that indicated the artificiality of the airstrike video — the evidence was excluded from the OHCHR report as unreliable. Ukraine, 2022-2023: the use of ML models to detect deepfake compositions in the content of Russian propaganda channels — the results were taken into account as part of the heuristic triage-filtering process of videos for UN investigative teams.	ICC: requires human retrospective examination (Rule 63 RPE); UN: used as an aid in fact-finding teams; ECHR: acceptable subject to fair trial and metadata verification.	Dorsey & Moffett [19]; Siraj, Jabbi, Budhiartie & Mustaffa [20]
Blockchain recording of evidence	Using a distributed ledger to provide cryptographic immutability, timestamping, and	Starling Lab, OpenArchive	Colombia, 2021: Starling Lab applied two-factor hashing (Merkle tree + IPFS-linking) to archive torture testimonies — prepared for submission to special jurisdictions of the	ICC: technologically promising, but requires expert certification; UN: currently not verified as an official channel;	Ponnusamy, Manickam & N, [21]; Loffi, Camillo, Souza,

Technology	Brief description	Implementation examples	Application precedents	Compliance with ICC / UN / ECHR standards	Academic research
	forensic tracing.		peace process. Ukraine, 2023: experimental blockchain encoding of evidence of missile strikes on Kharkiv — used as a forensic application in collaboration with the National Prosecutor's Office.	ECHR: may be part of an electronic digital dossier if it does not violate the right to protection.	Westphall & Westphall, [22]
Mobile testimonial apps	Applications with built-in cryptographic mechanisms for location/time binding, preserving the digital context of the event.	eyeWitness App, ProofMode	Myanmar, 2020: Evidence of mass burning of villages in Rakhine State was captured with GNSS metadata and audit logs — integrated into the IIIM database. Ukraine, 2022: eyeWitness App was used for field capture of artillery strikes in Sumy region — data exported with full set of hashes and digital authentication keys.	ICC: admissibility subject to data authentication; UN: full support within Human Rights Fact-Finding Missions; ECHR: may support evidence of violations of Articles 5, 6, 13 if metadata is properly preserved.	Divon & Eriksson Krutrök, [23]; Majeed, Abushbak, Qadri & Sinha [24]
Automated attribution systems	Platforms for identifying the source of generation, publication chain, server profile, and digital signature.	Google Verify, Project Origin	Syria, 2021: Google Verify provided server-side tracking of mass detention video attributed to government forces — confirmed by independent Human Rights Watch (HRW) audit. Ukraine, 2023: Microsoft Origin determined the infrastructure IP authenticity of a video of the execution of a Ukrainian prisoner of war — provided to the United Nations Mechanism for Ukraine (UNMHR).	ICC: used in the technical expertise (Rule 68); UN: recommended for use as part of the content evidentiary assessment process; ECHR: not an independent source, but supports the evidentiary base through verification of circumstances.	Perez-Leon-Acevedo [25]; Poole et al. [26]

Source: created by the authors

3.4. Instruments

The digital technologies for documenting war crimes were assessed according to two integral blocks of parameters: ethical and legal (procedural authenticity, adherence to the principles of a fair trial, protection of privacy) (Table 2); technological and legal (forensic reliability, metadata control, falsification resistance, interoperability, etc.) (Table 3).

Table 2: Ethical and legal block of parameters for the assessment of digital technologies for documenting war crimes

Parameter	Brief description
Evidence Admissibility	Compliance of the collected digital material with the admissibility criteria in accordance with Art. 69(4) of the Rome Statute, § 63 RPE (Rules of Procedure and Evidence of the ICC), Art. 6 of the ECHR.
Due process / fair trial	Guaranteeing compliance with the procedural rights of the parties, including the right to cross-examination of digital evidence and protection against biased algorithmic profiling.
Procedural Authenticity	The validity of provenance, chain of custody, and the integrity of the digital object (hash consistency, file integrity).
Deontological Legitimacy	Compliance with philosophical and legal criteria of moral legitimacy, in particular, avoiding re-traumatization and post-mortem exploitation of victims' data.
Right to Privacy / Data Protection	Compatibility of the technology with General Data Protection Regulation (GDPR), IHRL regulations, principles of purpose limitation, data minimization, and explicit consent.
Regulatory Congruity	Mutual compliance with the provisions of the ICC, UN, ECHR, UN FFM, IIIM, UNHRC, IHL.
Information ethics of publication	Taking into account the impact of content (especially visual) on public consciousness, avoiding visual trauma amplification, and abusing the status of evidence in information wars.

Source: created by the authors

Table 3: Technical and legal block of parameters for assessing digital technologies for documenting war crimes

Parameter	Brief description
Forensic Reliability	Verification of immutability of digital artifacts based on SHA-2/3, Merkle Root, blockchain timestamp, W3C-PROV provenance standards.
Chain of Custody Compliance	Evidential reconstruction of the audit trail, cryptographically signed event logs recorded in the system.
Source Attribution Validity	Establishing the origin of digital material through IP tracing, digital watermarking, server-side header logs, Content Provenance Architecture.
Tamper Resistance	Level of protection against deepfake interventions, metadata poisoning, semantic inversion, content spoofing.
Metadata Verifiability	Volume, accuracy and formalization of metainformation (EXIF, GPS, GNSS, XMP, JSON-LD) according to Digital Evidence ISO/IEC 27037:2012.
AI/ML Explainability & Triage	Level of explainability of verification systems (according to IEEE P7003, ALTAI Framework), heuristic filtering mechanisms, and automated reliability assessment.
Contextual Fragmentation Risk	The degree of loss of situational integrity of digital artifacts because of the lack of context, timestamping, connection to other sources (evidential disconnect).
Interoperability and Scalability	Compatibility with institutional databases (e.g. CIJA, UNMHR, I-Witness Database), capability for scalable integration into digital evidence ecosystems.

Source: created by the authors

The study used PlantUML (PlantUML, 2025) to formalize the architecture, component structure, and scenario procedural interaction of the elements of the framework of the global digital platform for documenting war crimes. PlantUML is a text-based modelling language that enables creating UML diagrams (of classes, sequences, components, etc.) by writing simple code. It supports automatic generation of visual diagrams from the description of interactions in the system.

4. RESULTS

A comparative analysis was conducted to provide a holistic understanding of the effectiveness of digital technologies for documenting war crimes. The analysis covered their legitimacy, ethical and deontological admissibility, ability to resist manipulation, and the extent of data fragmentation. The assessment is based on compliance with technical and forensic regulations, ICL norms (ICC), UN fact-finding procedures, and ECHR jurisprudence (Table 2, Table 3) – Table 4.

Table 4: Comparative analysis of digital technologies for documenting war crimes

Technology	Ethical and legal assessment	Technical and legal assessment	Applicability conclusion
OSINT	Limited admissibility (ICC 69(4)); partially complies with the fair trial principle; ethical dilemmas regarding secondary distribution of content without consent; potential violation of the right to privacy; regulatory congruence is unstable; information ethics — depends on the platform's moderation policy.	Forensic credibility depends on source verification; chain of authenticity is often broken; high fragmentation; limited semantic attribution; weak interoperability; low metadata control.	Suitable for preliminary attribution and open analysis, but requires further technical and legal validation.
GEOINT	High admissibility subject to proper attribution; complies with due process and privacy rights; regulatory congruence with OHCHR/UNOSAT; publication is usually governed by satellite operator standards.	High forensic reliability; precise chain of authenticity; semantic attribution provided by coordinates; resistant to falsifications; medium risk of fragmentation; high interoperability.	Recommended for strategic attack impact mapping and damage documentation with high evidentiality.
Digital evidence repositories	Full procedural authenticity; high level of data protection; meets ICC/UNITAD standards; information ethics built into data retention protocols.	Low risk of forgery; high level of metadata verification; perfect chain of authenticity; high interoperability; compliance with digital evidence standards.	Highest suitability for use in international law; recommended as the core of a digital evidence repository.
AI/ML verification systems	Admissibility depends on expert verification; requires transparency of AI process; risks of bias and unexplainability; right to privacy at risk; regulatory compliance is conditional.	High machine analytical efficiency; unstable semantic attribution; average falsification resistance; high interoperability; risk of uncontrolled fragmentation.	Effective as a heuristic triage tool, but requires expert support; risks of bias and opacity.
Blockchain-based evidence record	Theoretical compliance of the chain of custody; issues with legal legitimacy still open; respect for the right to	High level of tamper resistance; partial interoperability; requires verification of the chain of authenticity; metadata	Innovative, but requires legitimation; recommended for long-

Technology	Ethical and legal assessment	Technical and legal assessment	Applicability conclusion
	privacy - through cryptographic fixation; regulatory congruence depends on technology recognition by courts.	control is provided through a blockchain-based record.	term storage of evidence with crypto-confirmation.
Mobile evidence applications	High ethical admissibility; data authentication at the level of primary collection; meets legal requirements for privacy; integrates into protocols of human rights missions.	Low risk of fragmentation; reliable semantic attribution; full metadata control; high level of forensic credibility; optimal scalability.	Optimal for initial field recording of events; recommended for mobile human rights missions and real-time data collection.
Automated attribution systems	Admissibility as supporting evidence; meets the principle of due process only when checking logs and server traces; ethical risks — verification without the author's/victim's consent; partial regulatory compliance.	Average forensic reliability; verification relies on server-side analysis; weak metadata control; limited interoperability; suitable for correlative evidence analysis.	It is appropriate to use as an auxiliary element of attribution of digital sources; requires verification and legal registration.

Source: created by the authors

Comparative analysis (Table 4) showed that digital evidence repositories and mobile witness applications demonstrate the highest regulatory compliance, procedural authenticity and forensic reliability, ensuring the preservation of chain of custody and compliance with the principle of due process. GEOINT and OSINT platforms are characterized by high semantic attribution and interoperability, but need to be supplemented with tamper residency and metadata control mechanisms. AI/ML systems and automated attribution systems have limited deontological legitimacy because of the risks of analytical inversion and insufficient transparency of inference mechanisms. Blockchain-based record demonstrates the potential for traceological immutability, but requires further normative congruence with ICC and ECHR procedures.

Despite the fact that mobile witness applications have demonstrated the highest degree of operational relevance, as well as legal and procedural efficiency among the analysed digital technologies for documenting war crimes — in particular, in terms of evidentiary admissibility, chain of custody compliance, metadata control, ethical and deontological compliance, and procedural authenticity — their functionality remains limitedly encapsulated, segmented, and descriptive. The high risk of semantic fragmentation, the lack of modular interoperability, and the low level of automated heuristic triage indicate the structural incompleteness of such solutions in the context of large-scale documentation of jus in bello crimes.

So, there is a meta-analytic need for an architectural synthesis of a hybrid framework that accumulates forensically stable (blockchain), semantically attributed (OSINT), scalable (GEOINT), and machine-explainable (AI/ML) components. Such an integrative model should be based on normative and ethical stratification, legal congruence with the standards of the ICC, UN, ECHR, and meet the requirements of digital sovereignty of the evidentiary base. As a result, it is necessary to synthesize and model a global digital platform for documenting war crimes, capable of ensuring holistic evidentiary verification and trans-institutional evidentiary interoperability - Figure 2.

Journal of Theoretical and Applied Information Technology
31st October 2025. Vol.103. No.20

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

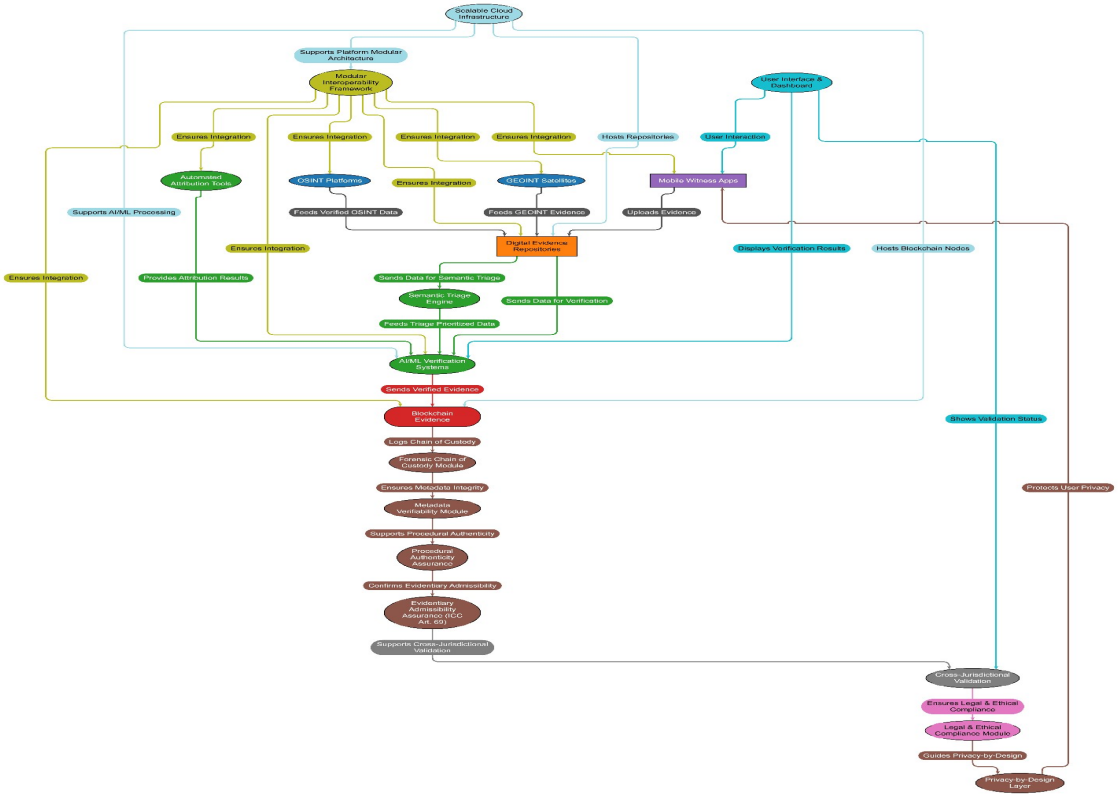

Figure 2: Synthesis concept of a framework for a global digital platform for documenting war crimes

Source: created by the authors

The synthesis concept of the Global Digital Platform for War Crimes Documentation Framework (Figure 2) is a modular, cloud-scale system that integrates OSINT platforms, GEOINT satellites, digital repositories, AI/ML verification systems, blockchain registration, mobile witness applications and automated attribution systems into a single evidentiary infrastructure. The system ensures full traceability of digital artifacts, chain of custody, and admissibility in accordance with Art. 69(4) of the Rome Statute, the ECHR and the UN protocols through semantic triage, forensic verification, metadata control, and blockchain anchors. Legal and ethical compliance is implemented through Privacy-by-Design, a compliance module and inter-jurisdictional validation, forming the basis for transterritorial use of evidence in international criminal law.

Given the complexity of the functional interaction between modules, the high degree of technological and legal interoperability, and the requirements for the normative and ethical stratification of the digital evidentiary ecosystem, the synthesis concept of the framework of the global digital platform for documenting war crimes requires formalized ontological modelling. The specified modelling method reflects the roles of components (agents), semantic dependencies (relations), procedural trajectories (workflows), and legal regulations (constraints) in the structure of digital verification - Figure 3.

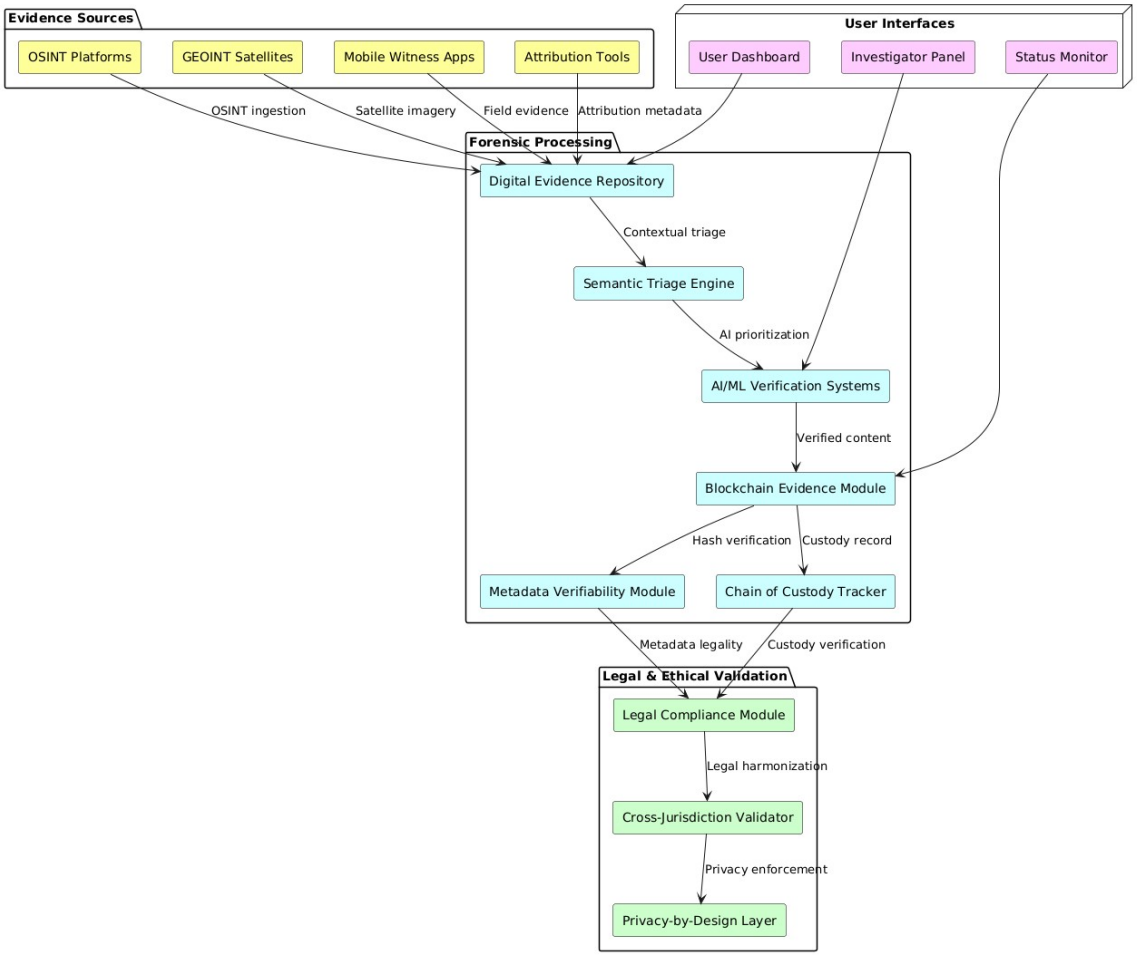

Figure 3: Component diagram of the synthesis concept framework for a global digital platform for documenting war crimes

Source: created by the authors in PlantUML [27]

The component diagram (Figure 3) reflects the architecture of the synthesis framework of the global digital platform for recording war crimes, which is structured according to four functional areas:

- Evidence sources (yellow): OSINT platforms, satellite intelligence, mobile applications, and attribution systems that ensure multi-format receipt of primary digital artifacts.
- Forensic processing (blue): repositories, AI/ML systems, blockchain modules and metadata verifiers that implement triage filtering, chain of authenticity preservation, and tamper resistance.
- Legal and ethical validation (green): modules for checking normative congruence, cross-jurisdictional admissibility, and privacy protection (ECHR, ICC, UN).
- User layer (pink): interfaces for researchers, analysts and monitoring bodies, integrated with all components of the platform.

The diagram demonstrates the logic of integrating digital technologies into a single evidentiary ecosystem with a focus on interoperability, reliability, and procedural admissibility.

The next stage of the research involves functional and procedural modelling to formalize the architectonics of a global digital platform for recording war crimes. This approach ensured traceability of information flows, identification of critical validation nodes, optimization of authenticity chain procedures, and verification of regulatory and legal compliance (ICC/ECHR/UN). The modelling allowed for the synthesis of multi-agent interaction of sources, processing modules, blockchain fixation, and legal filters into a coherent interoperable structure – Figure 4.

Journal of Theoretical and Applied Information Technology
31st October 2025. Vol.103. No.20

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

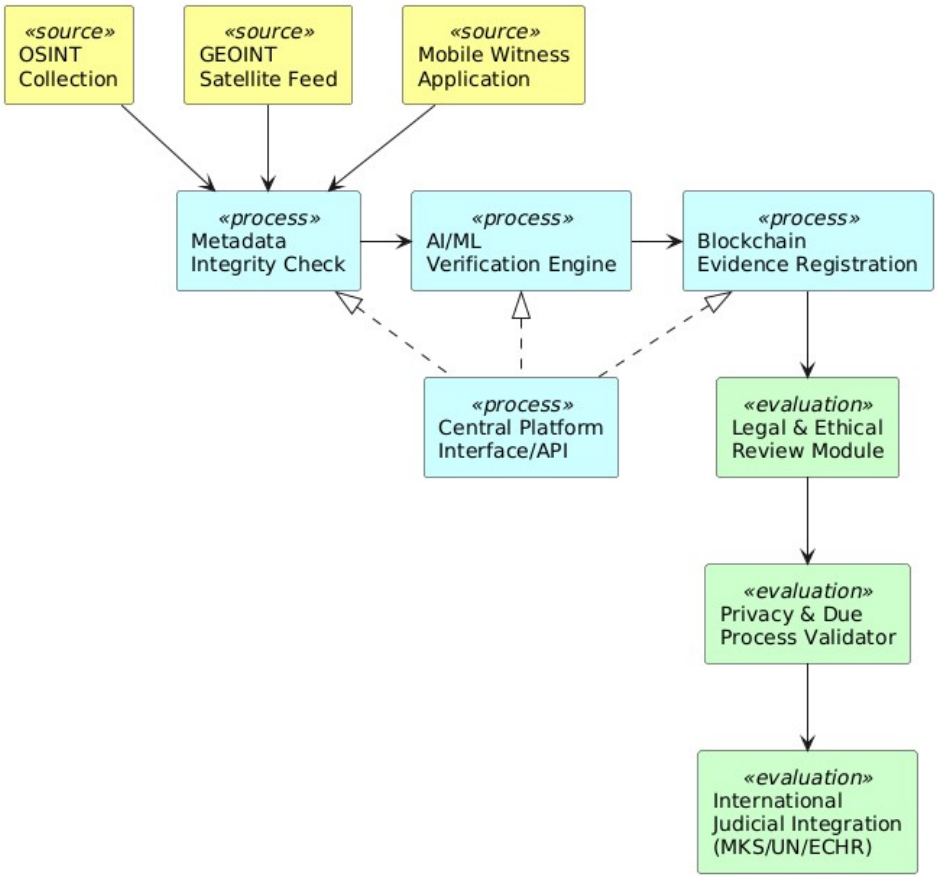

Figure 4: Functional and procedural modelling of the framework of a global digital platform for documenting war crimes

Source: created by the authors in PlantUML [27]

The results of the functional and procedural modelling of the global digital platform for documenting war crimes (Figure 4) demonstrate a multi-level architecture that integrates heterogeneous data sources (OSINT, GEOINT, mobile witness applications) with verification modules (metaintegration, AI/ML classification, blockchain registration) and regulatory control modules (due process compliance assessment, GDPR/ICCPR, admissibility review). The platform API component ensures interoperability and functional orchestration of processes through centralized control logic. The final stage of the model covers institutional integration with international structures (ICC, UN, ECHR), which ensures regulatory validity and judicial relevance of digital evidence.

Scenario sequence modelling is a key methodological tool for formalizing the interaction between digital evidence sources (OSINT, GEOINT, mobile applications), processing modules (AI/ML filtering, Blockchain-based record), regulatory verifiers (due process, privacy compliance), and users (investigators, human rights defenders). This approach provides procedural traceability, chain of custody simulation, forgery detection, data fragmentation detection, and interoperability of digital components within a framework that meets ICC, UN, and ECHR standards – Figure 5.

Journal of Theoretical and Applied Information Technology
31st October 2025. Vol.103. No.20

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

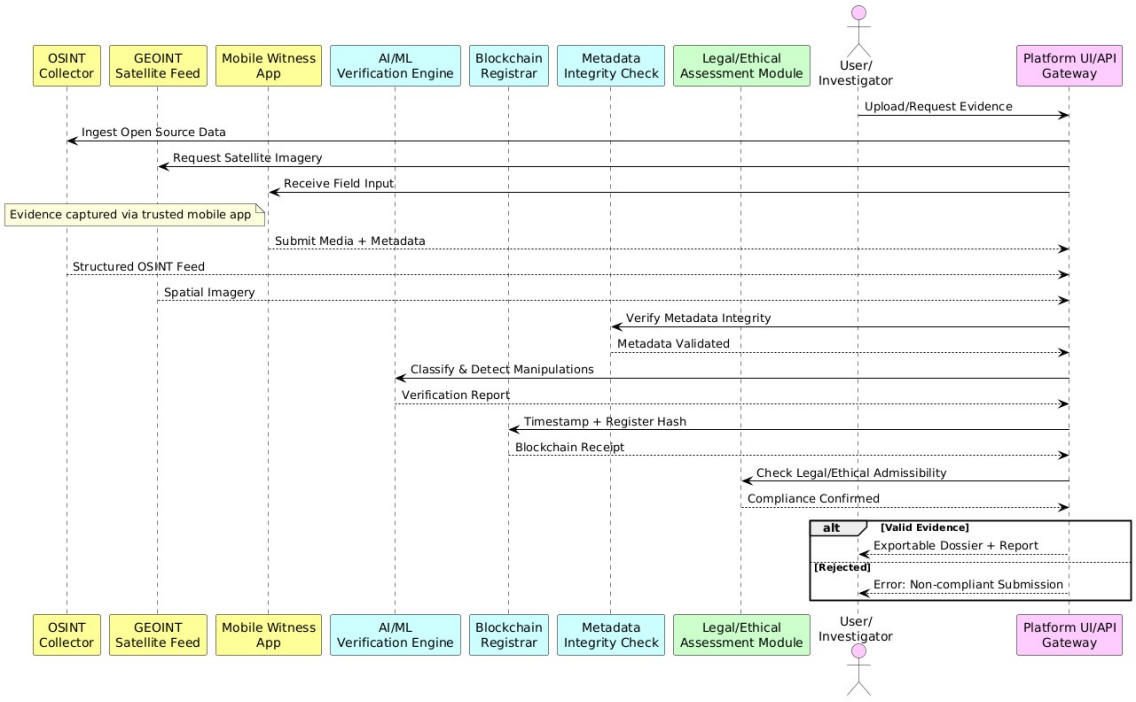

Figure 5: Scenario sequence modelling of the framework of a global digital platform for documenting war crimes

Source: created by the authors in PlantUML [27]

The model of scenario sequence interaction of the framework of the global digital platform for documenting war crimes (Figure 5) illustrates the step-by-step traceology of the evidentiary flow — from multi-source aggregation (OSINT, GEOINT, mobile applications) to legally verified presentation. The architecture includes the stages of semantic unification (structured feed), forensic validation of metadata, AI/ML discrimination of manipulations, registration on the blockchain (timestamp, hash-chain), as well as normative and ethical verification (due process, admissibility, privacy compliance). The verified result is formed as a digital dossier suitable for use in the ICC, UN or ECHR jurisdictions.

So, the developed framework of the global digital platform for recording war crimes is an integrative, forensically valid system that combines multi-source aggregation (OSINT, GEOINT, mobile witness applications), processing and verification modules (AI/ML, Blockchain, metadata-check), legal and ethical stratification (privacy, due process, admissibility), as well as institutional interoperability with international jurisdictions (ICC, ECHR, UN). The framework implements the principles of chain of custody, tamper-resistance, explainability, and legal traceability, which forms the basis for a globally standardized evidentiary infrastructure in the field of military law, ensuring relevance in the context of transitional justice, the functioning of post-conflict society, the protection of human rights, as well as the legal procedure of reparation of damages, in particular reparation for war-related damages.

5. DISCUSSION

The discussion section focuses on a comparative analysis of the framework developed during this study with relevant approaches representing the contemporary field of recording, verifying, and legal processing of digital evidence of war crimes. Particular attention is paid to conceptual differences, methodological innovations, and the level of forensic integration of the considered approaches.

The author [28] represents Twitter/X-archiving as an element of a mass digital epistemology of resistance, where OSINT cartography, transdisciplinary expertise, and digital political mobilization converge into a community-based structure of evidentiary advocacy. Instead, our study structures a verification platform based on procedural traceology, AI/ML discrimination,

blockchain registration, as well as normative ethical filtering, which ensures transjurisdictional admissibility of digital evidence in the forensic environment of international justice.

The author [29] identified the problem of incorporating online harms into the structure of international criminal law, considering them as new modes of committing core crimes (war crimes, crimes against humanity, genocide). Our study created a technological and procedural framework with AI/ML discrimination, blockchain fixation, and procedural traceology aimed at the forensic legitimation of digital artifacts and their admissibility in the transjurisdictional legal field.

The authors [30] established the ethical and methodological sustainability of military Telegram archives, considering semantic, visual, and link analytics as tools for studying digital epimerism. In contrast, our study formalizes a forensically validated framework with AI/ML filtering, blockchain logging and procedural traceology, focused on evidentiary admissibility and interjurisdictional congruence (ICC, ECHR).

The author [31] covered the practice of CCL as an actor-based model of documenting war crimes, combining OSINT research, field missions and advocacy verification within the scope of IHL. Instead, our study develops a technologically stratified framework with AI/ML filtering, blockchain logging and procedural traceology to enhance evidentiary integration.

The researcher [32] conceptualized the smartphone as an integral element of the sensor infrastructure of war, transforming the information operational participation of civilians and military personnel within an expanded ecosystem of digital surveillance and targeting. This study defines a forensic framework with AI/ML filtering, blockchain registration, and legal traceology, focused on evidentiary admissibility within the ICC, UN, and ECHR.

The author [33] explored the ethical and methodological specifics of oral history testimony collection using semi-structured interviews to reconstruct the everyday life of war and refugee Ukrainians. In contrast, this study structures a digital evidentiary ecosystem based on AI/ML filtering, blockchain-based record, and normative procedural traceology for the verification of war-related digital artifacts.

The author [34] interpreted gender-based violence through the lens of post-traumatic narratives and mass digitalization, using the case of Bosnia as a comparative framework. In turn, our study focuses on the techno-legal infrastructure of crime recording, institutionalizing digital evidence through AI/ML filtering, blockchain registration, and procedural traceology for legally relevant evidentiary purposes.

The authors [35] analysed OSINT practices of military eavesdropping through SDR resources, focusing on the network dynamics of data leakage, verification, and transformation into intelligence. In our study, these processes are institutionalized into an evidentiary framework with AI/ML filtering, blockchain logging, and procedural traceology, providing forensic validity for multi-level legal admissibility.

The researchers [36] presented the Lemkin Center as an institutional archival hub of humanitarian memory focused on the accumulation of evidence without the goals of procedural verification or judicial admissibility. In contrast, our study implements a forensic framework with AI/ML filtering, blockchain anchoring, and normative stratification for transjurisdictional evidentiary use.

The authors [37] identified four-vector functionality of the OSINT community (counterdisinformation, perceptual reconfiguration, military information, and crime documentation), emphasizing ethical and verification challenges. Our study systematizes these practices into a forensically validated framework with AI/ML filtering, blockchain-based record, and procedural traceology, institutionalizing OSINT as an evidentiary component of a transnational legal field.

The comparative discourse of the analysed studies demonstrated the diversity of approaches to the recording, archiving and institutionalization of military digital information — from epistemologies of digital resistance, OSINT cartography and humanitarian memory to refugee interviewing, platform analysis of Telegram/SDR and conceptualization of online harms. At the same time, the framework proposed in our study is distinguished by a systemic forensic stratification — AI/ML filtering, blockchain anchoring, regulatory tracing — that ensures the admissibility of digital evidence in transjurisdictional legal mechanisms, transforming disparate digital artifacts into procedurally valid objects of international criminal prosecution.

5.1. Limitation

A limitation of the study is the lack of empirical testing of the developed framework in real-world criminal procedures. Further validation of its operational effectiveness, evidentiary robustness, and transjurisdictional admissibility in the context of institutional implementation is necessary.

5.2. Recommendations

It is recommended to develop a pilot project with practical implementation of the framework in simulated criminal proceedings with the participation of relevant institutions. It is appropriate to carry out phased validation according to the criteria of procedural relevance, evidentiary integrity, and inter-jurisdictional consistency.

6. CONCLUSIONS

A comparative analysis of digital technologies for documenting war crimes revealed significant variability in their evidentiary capacity, depending on technological and procedural parameters. These include the degree of preservation of the chain of custody, the level of forensic reliability, semantic attribution, scalability, metadata control, falsification resistance, regulatory and legal congruence with the requirements of the ICC, UN, and ECHR. Digital evidence repositories and mobile witness applications showed the highest evidentiary stability, while AI/ML modules and automated attribution systems require regulatory refinement because of the risks of opacity of inference, bias effects, and limited explainability.

The optimal solution is the architectural synthesis of a hybrid framework that accumulates forensically validated (blockchain), semantically attributed (OSINT), regulatory protected (privacy-compliant), analytically explained (AI/ML) components within a transjurisdictional platform. Such a system provides legally relevant traceology of digital artifacts, their admissibility in criminal proceedings, supports institutional integration with international structures and meets the requirements of transitional justice, protection of human rights, reparation of damages, including reparation for war-related damages, in the context of the functioning of a post-conflict society.

The proposed framework for digital documentation of war crimes aims not only at technically optimizing the collection and verification of evidence, but also performs an important function in shaping the rule of law, guaranteeing the protection of human rights, and supporting the formation of civil society. These aspects are key in the framework of transitional justice, which involves the restoration of justice, restitution to victims, and international legal responsibility for violations of jus in bello.

Our analysis highlights not only the differentiated evidentiary robustness of digital tools but also underscores the critical need for an interoperable, forensically validated, and legally stratified architecture capable of meeting the procedural rigour of jus in bello enforcement. We argue that the proposed hybrid framework offers more than technological optimisation: it establishes a foundational infrastructure for ensuring chain of custody, admissibility, and legal traceability across jurisdictions. This work contributes to advancing transitional justice, enabling post-conflict societal resilience, and operationalising digital accountability through scalable, rights-oriented solutions.

The academic novelty of the research is the formalisation of a multi-agent forensic legal framework of a global digital platform for documenting jus in bello crimes, which integrates blockchain-based records, AI/ML modules of semantic discrimination, OSINT/GEOINT aggregation, metadata control modules, and regulatory stratification (ICC, ECHR, UN). The study is the first to propose an ontological model of inter-component interaction, taking into account the principles of chain of custody, tamper-resistance, explainability, and admissibility, which ensures the coherence of the digital evidentiary ecosystem with transjurisdictional admissibility.

The practical significance of the research results is the developed structured digital architecture suitable for implementation in the practice of international criminal justice for documenting war crimes. The proposed framework can be used as a prototype for creating standardised tools for collecting, processing, verifying, and preserving digital evidence with high evidentiary stability. It can also be adapted to the needs of monitoring, human rights and judicial bodies in the context of hybrid armed conflicts, taking into account the requirements of transitional justice, restoration of human rights, reintegration of post-conflict society and mechanisms for compensation for damages, in particular those caused by military operations.

REFERENCES:

[1] S. Allan, “Visual War Journalism”, *Digital Journalism*, 2025, pp. 1–17. doi:10.1080/21670811.2024.2443153

[2] J. Kotišová & L. van der Velden, “The Affective Epistemology of Digital Journalism: Emotions as Knowledge among On-the-ground and OSINT Media Practitioners Covering the Russo-Ukrainian War”, *Digital Journalism*,

2025, pp. 1–20. doi:10.1080/21670811.2023.2273531

[3] K. Gavrysh, "Digital Evidence in the Practice of the International Criminal Court: What Future for Proceedings on War Crimes Committed in Ukraine?", In: *Global Issues*. Cham: Springer Nature Switzerland, 2025, pp. 107–129. doi:10.1007/978-3-031-84216-0_6

[4] K. Maruma, "The Crucial Role of Evidence and Witness Testimony in International Criminal Court War Crimes Prosecutions", *Journal of Humanities and Education Development*, Vol. 7, No. 2, 2025, pp. 36–46. doi:10.22161/jhed.7.2.5

[5] M. Ochi & H. Dagenborg, „Online War-Crime Archives: A Call for a Universal Guideline", Available at SSRN 5128953, 2025. doi:10.2139/ssrn.5128953

[6] V. Santini, "Visual Representation of Armed Conflict-Related Deaths and the Evolving Standards of Protecting the Dignity of the Deceased", *International Review of the Red Cross*, 2025, pp. 1–22. doi:10.1017/s1816383125100593

[7] J. Peake, "Challenges of Using Digital Evidence for War Crimes Prosecutions: Availability, Reliability, Admissibility", *AJIL Unbound*, Vol. 118, 2024, pp. 57–61. doi:10.1017/aju.2024.5

[8] P. Kulikov, O. Aziukovskyi, O. Vahonova, O. Bondar, L. Akimova, O. Akimov, "Post-War Economy of Ukraine: Innovation and Investment Development Project", *Economic Affairs (New Delhi),* Vol. 67, No. 5, 2022, pp. 943-959.

[9] T. Al-Billeh, A. Al-Hammouri, T. Khashashneh, M. Al Makhmari & H. Al Kalbani, "Digital Evidence in Human Rights Violations and International Criminal Justice", *Journal of Human Rights, Culture and Legal System*, Vol. 4, No. 3, 2024, pp. 842–871. doi:10.53955/jhcls.v4i3.446

[10] P. Grzebyk & D. Uczkiewicz, „The Russian-Ukrainian Conflict and War Crimes: Challenges for Documentation and International Prosecutio", London: Routledge, 2024. doi:10.4324/9781003493785

[11] D.S. Melnyk, O.A. Parfylo, O.V. Butenko, O.V. Tykhonova, V.O. Zarosylo, "Practice of the Member States of the European Union in the Field of Anti-Corruption Regulation", *Journal of Financial Crime,* Vol. 29, No. 3, 2022, pp. 853-863. doi:10.1108/JFC-03-2021-0050

[12] H. Kuczyńska, "Digital Evidence in Investigations Concerning Russian Crimes in Ukraine", In *The Russian-Ukrainian Conflict and War Crimes*. London: Routledge, 2024, pp. 129-144. doi:10.4324/9781003493785-10

[13] T. Dodds, L. van der Velden, G. Torres, A. El-Masri, S. D. Reese, G. Fiorella, J. Kotišová, "On the Institutionalization of OSINV in Journalistic Practice", *Journalism & Mass Communication Quarterly*, 2025. doi:10.1177/10776990251334382

[14] N. Flamer, "Hizballah's Intelligence Collection Leading Up to and during the 2006 War with Israel: How a VNSA Conducts Operative Intelligence", *Terrorism and Political Violence*, 2025, pp. 1–17. doi:10.1080/09546553.2025.2508799

[15] Riefda Novikarany, "Geoint as a Driver of National Security", *International Journal of Scientific Multidisciplinary Research*, Vol. 3, No. 2, 2025, pp. 237–250. doi:10.55927/ijsmr.v3i2.66

[16] R. Dickey & M. P. Gleason, "Space and War in Ukraine: Beyond the Satellites", *Æther: A Journal of Strategic Airpower & Spacepower*, Vol. 3, No. 1, 2024, pp. 20-35.

[17] C. Rose, "Evidentiary Challenges in the Litigation of War Reparations: Armed Activities on the Territory of the Congo (DRC v Uganda)", *Journal of International Dispute Settlement*, Vol. 16, No. 1, 2025, idaf004. doi:10.1093/jnlids/idaf004

[18] A. Florczak, A. Jach & J. Rosłon-Żmuda, „The Role of States and International Organisations in Bringing War Crimes to Account in the Context of the Russian-Ukrainian War", In: *For Security and for Peace.* London: Routledge India, 2024, pp. 83–103. doi:10.4324/9781003558040-8

[19] J. Dorsey & L. Moffett, "The Warification of International Humanitarian Law and the Artifice of Artificial Intelligence in Decision-Support Systems: Restoring Balance through the Legitimacy of Military Operations", *SSRN Electronic Journal*, 2025. doi:10.2139/ssrn.5239131

[20] A. Siraj, Y. Jabbi, A. Budhiartie & A. Mustaffa, "Redefining Accountability: Ai's Role in Prosecuting Transnational Crimes under International Law", *Audito Comparative Law Journal (ACLJ)*, Vol. 6, No. 2, 2025, pp. 124–145. doi:10.22219/aclj.v6i2.40434

[21] V. Ponnusamy, N. Manickam & N. Arivazhagan, „Blockchain Technology for Evidence Integrity", In: *Forensic Intelligence and Deep Learning Solutions in Crime Investigation*. Hershey: IGI Global, 2025, pp. 23-42. doi:10.4018/979-8-3693-9405-2.ch002

[22] L. Loffi, G. L. Camillo, C. A. D. Souza, C. M. Westphall & C. B. Westphall, "Management of the Chain of Custody of Digital Evidence Using Blockchain and Self-Sovereign Identities: A Systematic Literature Review", *IEEE Access*, Vol. 1, 2025. doi:10.1109/access.2025.3560191

[23] T. Divon & M. Eriksson Krutrök, "The Rise of War Influencers: Creators, Platforms, and the Visibility of Conflict Zones", *Platforms & Society*, Vol. 2, 2025. doi:10.1177/29768624251325721

[24] T. Majeed, A. M. Abushbak, M. Qadri & A. Sinha, "Cross-National Civilian Reporting of the Everydayness of War: Emerging Citizen Journalism Practices in Palestine and Kashmir", *Journalism*, Vol. 26, No. 5, 2024. doi:10.1177/14648849241273581

[25] J. P. Perez-Leon-Acevedo, "Rethinking Attribution Standards for State Responsibility Concerning Mass Atrocities", *San Diego International Law Journal*, Vol. 26, No. 2, 2025, p. 179.

[26] D. N. Poole, D. Andersen, N. A. Raymond, J. Parham, C. Howarth, O. A. Hathaway & K. Khoshnood, "The Effect of Conflict on Damage to Medical Facilities in Mariupol, Ukraine: A Quasi-Experimental Study", *PLOS Global Public Health*, Vol. 5, No. 1, 2025, p. 0003950. doi:10.1371/journal.pgph.0003950

[27] PlantUML, 2025. URL: https://plantuml.com/

[28] S. Seegel, "Geopolitical Frames, Bold Lines: Online Global Solidarity and Mapping Russia's War Against Ukraine", *On_Culture*, Vol. 18, 2025. doi:10.22029/oc.2025.1508

[29] S. Zarmsky, "Is International Criminal Law Ready to Accommodate Online Harm?", *Journal of International Criminal Justice*, Vol. 22, No. 1, 2024, pp. 169-184. doi:10.1093/jicj/mqae013

[30] M. Bareikytė, M. Makhortykh, A. Martin, T. Nazaruk & Y. Skop, „How Should Platforms Be Archived? On Sustainable Use Practices of a Telegram Archive to Study Russia's War against Ukraine", *Media, Culture & Society*, Vol. 46, No. 7, 2024. doi:10.1177/01634437241245915

[31] R. Nekoliak, "The Center for Civil Liberties", In: *The Russian-Ukrainian Conflict and War Crimes*. London: Routledge, 2024, pp. 159–175. doi:10.4324/9781003493785-12

[32] M. Ford, "From Innovation to Participation: Connectivity and the Conduct of Contemporary Warfare", *International Affairs*, Vol. 100, No. 4, 2024, pp. 1531–1549. doi:10.1093/ia/iiae061

[33] A. Wylegała, "Ethical and Methodological Challenges of Documenting the War", In: *The Russian-Ukrainian Conflict and War Crimes*. London: Routledge, 2024, pp. 145-158. doi:10.4324/9781003493785-11

[34] N. Mocnik, "Empowering New Survivors with Old Lessons? Insights from the Bosnian War Aftermath Applied to Upcoming Ukrainian Post-Realities", *Canadian Slavonic Papers*, Vol. 66, No. 1-2, 2024, pp. 107–129. doi:10.1080/00085006.2024.2363164

[35] A. van Harten, S. Donnelly, P.-T. de Boer & R. van Rijswijk-Deij, "Expertise Hubs and the Credibility Challenge for Open-Source Intelligence: Insights from Usage Patterns of a Web-Controlled Radio Receiver and Related Twitter Traffic in the Ukraine War", *European Security*, 2024, pp. 1–21. doi:10.1080/09662839.2024.2421262

[36] A. Konopka & K. Wiciarz, „Witnesses to the War", In: *The Russian-Ukrainian Conflict and War Crimes*. London: Routledge, 2024, pp. 176–192. doi:10.4324/9781003493785-13

[37] H. van Beek & S. Rietjens, "Open-Source Intelligence in the Russia-Ukraine War", In: *Reflections on the Russia-Ukraine War*. Leiden: Leiden University Press, 2024, pp. 57–76. doi:10.24415/9789400604742-005