Use of Modern Information Technologies in the Investigation of War Crimes

Olena Melnikova [1], **Andrii Kuntii** [2], **Nataliia Prodanets** [3], **Dmitry Snitnikov** [4], **Ihor Fedorov** [5], **Liudmyla Kryvda** [6]

[1] Department of Criminal Law Disciplines, Odesa State University of Internal Affairs, Odesa, Ukraine
[2] Department of Criminal Law and Procedure, Leonid Yuzkov Khmelnytskyi university of management and law, Khmelnytskyi, Ukraine
[3] Department of Criminal Law Disciplines Odesa State University of Internal Affairs Odesa, Ukraine
[4] Department of Criminal Law Disciplines, Odesa State University of Internal Affairs, Odesa, Ukraine
[5] Department of Criminal Law Disciplines, Odesa State University of Internal Affairs, Odesa, Ukraine
[6] Department of Criminal Procedure and Criminalistics, Odesa State University of Internal Affairs, Odesa, Ukraine

The article develops a legal and applied framework for the use of modern information technologies in the investigation of war crimes under Chapter XIX of the Criminal Code of Ukraine, with a focus on wartime standards for the collection, verification and preservation of digital evidence. The methodology integrates criminalistics, digital forensics, OSINT, satellite imagery, criminal analytics platforms and Artificial Intelligence tools to ensure the reproducibility of results, procedural integrity and an unbroken chain of custody. Particular attention is paid to open-source verification techniques, the evidentiary value of satellite data, and the procedural compatibility of analytical systems (including Analyst's Notebook and Maltego) with judicial requirements for admissibility. The article substantiates that the implementation of ISO/IEC 27037:2012, standardized investigative protocols, secure interoperable databases and transparent AI auditing is essential for ensuring the reliability, resilience and international accountability of war crime investigations in conditions of armed conflict.

Keywords: war crimes, investigation, digital evidence, OSINT, satellite imagery, criminal analysis, remote monitoring, artificial intelligence, verification, chain of custody.

1. Introduction

Ensuring national security, stable functioning of the political and economic systems of the state presupposes the presence of an effective mechanism for combating criminal activity in the military sphere, as well as the legal consolidation of the corresponding regime of its functioning. In conditions of armed conflict, such measures acquire paramount importance, since they are aimed at protecting state sovereignty, territorial integrity and security of citizens. Amendments to the Criminal Code of Ukraine (hereinafter referred to as the Criminal Code of Ukraine) are due to the need for adequate and timely response of legislation to new challenges and threats to the state.

The implementation of military-legal reform in Ukraine has brought to the forefront a number of theoretical and practical tasks for domestic legal science that require thorough research. Among them is the improvement of legal regulation of the activities of the Armed Forces of Ukraine, in particular, taking into account the role of officials vested with command, organizational and administrative powers. The legislation requires that these powers be used exclusively for the benefit of military service. In the event of committing a crime while on duty, such persons violate the requirements of Article 17 of the Constitution of Ukraine, the laws of Ukraine, and the Military Oath, which provides for the conscientious and honest performance of military duty [1].

The current military-political situation in Ukraine, in particular the ongoing armed aggression of the Russian Federation, creates an increased level of threats to state security, which requires

constant high combat readiness of the Armed Forces, protection of state borders, and physical security of the population. The military conflict has shown that the usual organizational forms of activity of military justice bodies and the procedure for investigating criminal offenses during active hostilities become unacceptable. Therefore, there is a need to create new regulatory and procedural prerequisites to ensure the effectiveness of the investigation of crimes in the military sphere [2].

At the procedural level, the investigation of war crimes is carried out in accordance with the Criminal Procedure Code of Ukraine, which establishes the principles of criminal proceedings, the powers of pre-trial investigation bodies, prosecutors and investigating judges, as well as regulates the use of technical means, electronic information systems and digital evidence during criminal proceedings, including under conditions of martial law [3].

The extreme conditions of martial law require the use of modern approaches to the detection and investigation of war crimes, in particular through the integration of the achievements of legal science and forensics. In this context, it is relevant to study the negative factors that affect the process of investigating criminal offenses committed by military personnel, as well as to identify ways to improve criminal law regulation in this area.

The purpose of this article is a comprehensive study of the possibilities of using modern information technologies in the process of investigating war crimes, provided for by Chapter XIX of the Criminal Code of Ukraine, taking into account national and international standards for collecting, recording, analyzing and preserving digital evidence.

2. Literature review

The problem of investigating war crimes, provided for by Chapter XIX of the Criminal Code of Ukraine, received a new impetus for development after the start of large-scale armed aggression against Ukraine. Scientists are increasingly turning to interdisciplinary approaches that combine criminal law, international humanitarian law, forensics and information technologies.

In domestic science, certain aspects of the digitalization of the evidence process have been studied, in particular, by O. Kaplina, who justifies the importance of electronic evidence as a tool for restoring justice in armed conflicts [4]; M. Khavronyuk, who emphasizes the importance of technological adaptation of investigative activities to the conditions of martial law [5]; O. M. Kostenko, who considers the issue of war crimes through the prism of human rights and digital security [2].

In foreign doctrine, the approach to the use of modern information technologies as a way to ensure objectivity, reliability and transparency of the investigation of international crimes dominates. Modern technologies of remote monitoring, satellite imagery analysis and open source information (OSINT) are increasingly used as supporting tools for the International Criminal Court and national justice authorities to capture evidence of war and military crimes [6; 7]. Thus, S. Higgins in his work Truth in a Digital Age: The Role of Open Source Investigations in International Criminal Justice emphasizes that digital evidence obtained through OSINT platforms can significantly increase the level of transparency and accountability in cases considered by international tribunals [7]. At the same time, A. Smeulers emphasizes that the effectiveness of digital forensics in recording facts of violations of international humanitarian law depends on the unification of methods for collecting and verifying electronic data [8].

Another important area of development is the standardization of approaches to verifying digital evidence in international criminal justice, as reflected in reports and analytical reports prepared under the auspices of the Berkeley Center for Human Rights and the Institute for the Future [6; 8]. Such approaches are useful for national law enforcement agencies, including when documenting war crimes under Chapter XIX of the Criminal Code of Ukraine, which requires high standards of digital authenticity and data security.

Despite this, a systematic analysis of the use of modern information technologies in the investigation of war crimes committed in the context of an international armed conflict on the territory of Ukraine is still insufficiently developed in the scientific literature. There is a need to study the

legal, organizational and technical aspects of integrating information technologies into the activities of law enforcement agencies, as well as to determine their potential in proving the elements of crimes stipulated by Chapter XIX of the Criminal Code of Ukraine.

3. Methodology

To study the use of modern information technologies in the investigation of war crimes, a comprehensive interdisciplinary approach was applied, combining methods of criminal law, criminology and digital forensics. A qualitative analysis of Ukrainian legal acts and international standards, in particular Chapter XIX of the Criminal Code of Ukraine, ISO/IEC 27037 and the practices of the International Criminal Court, was used. A systematic review of scientific publications by domestic and foreign authors on the use of ICT, OSINT, satellite intelligence and criminal analytics tools in military conflicts was conducted. A comparative method was applied to determine the features of the legal regulation of war crimes in different jurisdictions and the effectiveness of digital evidence. The case study methodology was used to analyze practical examples of the use of ICT during the investigation of war crimes in Ukraine. In addition, an expert survey of specialists in the field of criminal law and digital security was conducted to assess the relevance and effectiveness of the proposed technologies. The method of logical analysis and synthesis was used to process and systematize data, which allows identifying cause-and-effect relationships between technological tools and investigation results. Such a multi-level approach allowed for a comprehensive assessment of the potential of modern technologies in increasing the evidentiary value, transparency and efficiency of the analyzed criminal proceedings.

4. General characteristics of war crimes

As is known, the main task of the Armed Forces of any state is to protect its sovereignty, territorial integrity and protect the country from acts of aggression by other states (external danger), as well as within its own state borders – from internal threats, such as the activities of terrorist groups or separatist movements. The creation, support and functioning of the armed forces is not only the right of the state, but also a necessary condition for ensuring its independence and the realization of national interests.

The armed forces as a power institution of the state arose simultaneously with the formation of the first state formations. It was then that the need arose for the legal regulation of the responsibility of persons in military service for committing unlawful acts, which are now classified as war crimes. These offenses constitute a complex and heterogeneous set of actions or inactions that encroach on the established order of military service. Their increased social danger lies not only in the violation of law and order, but also in the undermining of military discipline - an important condition for the combat readiness of the armed forces and other military formations.

In most countries of the world, military criminal law is a separate branch of national legislation. The exception is states that historically developed within the Soviet legal system or had a related tradition (in particular, the former republics of the USSR, Yugoslavia, Bulgaria, Hungary, the People's Republic of China, Vietnam, Mongolia, Poland, Romania, the Czech Republic, Sweden), where the norms on war crimes are integrated into criminal codes in the form of separate sections or paragraphs.

In states where the provisions of military criminal law are part of the criminal code, the legislator usually defines the legal concept of a war crime or a crime against military service. They do not have fundamental differences from the concept enshrined in Article 401 of the Criminal Code of Ukraine. This article is a unique norm of the Special Part of the Criminal Code of Ukraine, as it contains a generic definition of crimes against the established procedure for performing military service – in fact, the only generic definition of a criminal offense enshrined at the level of the law.

According to Part 1 of Article 401 of the Criminal Code of Ukraine, war crimes are recognized as criminal offenses against the established procedure for performing or completing military service,

committed by military personnel, as well as conscripts and reservists during their training. This provision is universal in nature and applies to all categories of crimes provided for within Section XIX of the Special Part of the Criminal Code of Ukraine.

The inclusion of military criminal law norms in the unified Criminal Code has a positive effect, as it ensures convergence with the norms of general criminal law and the implementation of the principle of legality in the field of criminal law regulation of military service.

The system of military crimes in Ukraine is formed by 34 articles (Articles 401–435 of the Criminal Code of Ukraine). Depending on the direct object of the offense, scientists (Anisimov and others,) divide them into the following main groups: crimes against the order of subordination and military dignity - disobedience (Article 402), failure to comply with an order (Article 403), resistance to a superior (Article 404), threat or violence against a superior (Article 405), violation of statutory rules of relations (Article 406); crimes against the order of military service – unauthorized leaving of a military unit (Article 407), desertion (Article 408), evasion of military service (Article 409); crimes against the order of preservation of military property – theft, appropriation or damage to military property (Articles 410–413); crimes against the order of operation of military equipment – violation of the rules of handling weapons, operation of machines, flights, ship navigation (Articles 414–417); crimes against the order of combat duty and special services – violation of the rules of guard, border or combat service (Articles 418–421); crimes in the field of protection of state secrets – disclosure or loss of military information (Article 422); military official crimes – negligent attitude to service, inaction of military authorities (Articles 425–426); crimes in a combat situation – leaving the battlefield, voluntary surrender, looting, etc. (Articles 427–432); crimes stipulated by international conventions – violence against the population in the area of combat operations, mistreatment of prisoners of war, illegal use of the Red Cross symbols (Articles 433–435).

Such a division of war crimes is appropriate, since it takes into account the direct object of the offense. The generic concepts of crimes stipulated in the sections of the Special Part of the Criminal Code of Ukraine are doctrinal, that is, they perform the function of scientific and logical abstractions that help in the knowledge of social and legal phenomena. The exception is the enshrining in the law of the generic concept of crimes against the established procedure for military service.

In view of this, only military personnel, conscripts, and reservists during training can be subjects of war crimes. Civilians are not subject to liability under military articles, except in cases of complicity [9].

5. The role of information and communication technologies in the system of proving war crimes

In modern conflicts, information and communication technologies (hereinafter referred to as ICTs) have become key in proving war crimes, since most events occur or are recorded in a digital environment. Photo and video materials, metadata, electronic messages, publications on social networks form a digital “trace base” that allows you to recreate the chronology of events, establish temporal and spatial correlations and personify the actions of specific subjects. These factors make ICTs an integral element of the system of evidence in war crimes cases [10].

However, the mere fact of the presence of a digital trace does not ensure automatic judicial admissibility of such evidence. Compliance with the procedures for recording, collecting, identifying and preserving information is key. Only strict adherence to the principles of digital forensics – in particular, documenting actions, protecting the chain of custody and using certified collection tools – guarantees the validity of digital evidence in court.

In a war zone, this process is complicated by the lack of secure access to the scene, the destruction of infrastructure, and the risk of data compromise due to cyberattacks or enemy information operations. In this regard, some researchers emphasize the need to adapt forensic protocols to wartime conditions: the introduction of mobile data collection systems, secure information transmission channels, and immediate verification of metadata [11].

International standards, such as ISO/IEC 27037, establish unified requirements for the processes of identification, collection, and preservation of digital evidence. The document emphasizes the importance of maintaining detailed documentation, labeling of media, and maintaining a complete history of actions with digital files, which is critically important in the context of armed conflicts [12].

No less significant is the issue of the reliability of digital sources. In the era of disinformation campaigns, deepfakes, and metadata manipulation, it is necessary to combine technical methods of detecting fakes with procedural guarantees of the chain of evidence. The practice of journalistic and research OSINT groups, such as Bellingcat, demonstrates that verifying data through geolocation, shadow analysis, and cross-checking with independent sources increases their evidentiary reliability [13].

From a methodological point of view, digital sources should be considered not as separate files, but as elements of a complex information system. This involves the integration of criminalistics, digital forensics, expert analysis, and the norms of international criminal law. Synchronizing these areas allows not only to identify individual episodes, but also to restore the general context of the crime, establish motives, subjects, and mechanisms of their actions.

An important practical aspect is the proper training of specialists capable of working with digital evidence in real combat conditions. Without a trained network of investigators, prosecutors and experts, even the most modern technologies will not be able to provide the proper level of evidence. Therefore, it is advisable to develop national training protocols and regularly improve the skills of personnel.

It can be argued that the effectiveness of the use of ICT in proving war crimes is determined by a combination of three factors: technical infrastructure, regulatory and procedural support and the human factor. Only their integration allows achieving the necessary level of transparency, reliability and legal stability of digital evidence [10].

A promising direction of development is the development of national procedures for adapting international standards to Ukrainian wartime realities, improving methods for rapid transmission and verification of digital data, as well as creating interdepartmental platforms for the secure exchange of evidence. Such an approach will contribute to improving the quality of investigations and strengthening trust in the results of criminal prosecution of war crimes.

6. Use of Open Source Technologies (OSINT) and Satellite Intelligence

In modern conditions of armed conflicts, the use of Open Source Technologies (OSINT) and satellite intelligence is becoming increasingly important for documenting violations classified as war crimes under Chapter XIX of the Criminal Code of Ukraine. The availability of digital traces – photo and video materials, posts on social networks, satellite images – creates a new ecosystem of evidence in which traditional investigative methods are supplemented and often replaced by open sources. The point is not only to collect information, but also to properly verify it, form a spatio-temporal context and integrate it into the criminal legal process.

Monitoring social networks allows you to quickly identify events that can be characterized as war crimes: for example, posting geotagged photos or videos accompanied by comments or reposts that allow you to establish the time, place and participants of the incident. Further, the following data are subject to analysis: metadata extraction, authentication, geolocation of frames, moving timelines of events. For example, analytical systems use social media data in combination with OSINT tools to detect military equipment, its location and movement during hostilities [14].

Satellite imagery performs the function of an “external third witness”: high- and medium-resolution images allow documenting the consequences of attacks, the destruction of civilian and military infrastructure, mass burials, and the movement of military equipment columns. Such data are important for war crimes investigations – they provide a temporal and spatial panorama that is difficult to falsify without significant costs.

International practice indicates the active use of OSINT methods in the processes of

investigating war crimes. Organizations such as Bellingcat and UNITAD use open sources, satellite imagery, and social media research to identify perpetrators, establish circumstances, and support the evidentiary process [15]. This use sets a precedent for OSINT technologies to become a separate evidentiary channel in international and national courts.

However, the use of OSINT and satellite data in criminal proceedings is accompanied by a number of legal and procedural challenges. For example, it is necessary to ensure the chain of custody of evidence, take into account the requirements for the admissibility of evidence before national courts, and also address the issues of authenticity and integrity of digital materials. Publications by Ukrainian scientists warn of the risk that open source data can be manipulated or intentionally distorted by the aggressor, which is why they need to be verified and combined with traditional investigative methods [14].

The key methodological step is to create a comprehensive analysis system that combines OSINT, geolocation, satellite intelligence, and traditional criminal investigation approaches. Such a system should include: (1) an automated or semi-automated open data collection platform; (2) metadata verification and georeferencing procedures; (3) integration of the obtained data into the criminal-legal context - that is, comparison with the qualification of crimes under Chapter XIX of the Criminal Code of Ukraine and preparation of the evidence base for trial. As a result of this approach, the reliability and efficiency of investigations are increased.

In practice, cases have already been implemented in Ukraine where OSINT analytics has become part of state and public investigation: in particular, the introduction of mobile applications for reporting crimes, geotagging of photos/videos of witnesses, as well as cooperation with volunteer analysts. These practices indicate that open sources can mobilize society to collect evidence, and then transfer it to official investigative bodies.

At the same time, it is worth paying attention to the ethical, security and legal limitations of such technologies: the risk of personal data leakage, danger to witnesses, the possibility of counter-disinformation and attribution of evidence. Ignoring these aspects can lead to rejection of evidence or harm to victims. Thus, the introduction of OSINT technologies in the investigation of war crimes must be accompanied by appropriate security policies and protection standards.

Thus, open source and satellite intelligence technologies play a revolutionary role in proving war crimes: they allow for the prompt recording, verification and interpretation of digital traces that were previously inaccessible or difficult to use. However, their effectiveness largely depends on the correct procedural and regulatory support - integration into criminal proceedings, compliance with evidentiary procedures under Chapter XIX of the Criminal Code of Ukraine and international standards. It is such a combined approach that can ensure proper judicial admissibility and fairness in bringing war crimes to justice.

7. Criminal Analysis Tools in a Military Context

In a military context, the investigation of war crimes becomes complex, requiring the use of criminal analytics systems, such as i2 Analyst's Notebook, Palantir Gotham, Maltego. These tools allow you to aggregate large data sets, visualize connections between subjects, events, and objects, and establish temporal and spatial patterns, which is critically important for the qualification of crimes under Chapter XIX of the Criminal Code of Ukraine.

Criminal analytics systems provide investigators with the opportunity to create network models of connections – for example, which of the individuals supervised the logistics of the military units that committed the crime, what were the movement routes, what supplies were made, etc. Such visualization helps to substantiate the participation of a specific person or group in the crime, establish cause-and-effect relationships, and identify patterns that previously remained hidden.

Temporal and spatial analyses become crucial precisely in the context of military operations: when, where, and under what circumstances atrocities occurred, whether they were systematic or random. The instrumental possibility of constructing timelines and geo-mapping allows us to investigate, for example, why certain areas became the object of intensive attacks, whether military

formations were moved to the places of crimes, and whether there was an interdependence between logistics and operational actions. This approach significantly improves the ability to justify the qualification of a crime as a crime under Chapter XIX of the Criminal Code of Ukraine [16].

The creation of integrated databases of war crimes is another key component. Such a database can collect data on events, subjects, locations, material traces, satellite images, video and photo metadata, and OSINT service reports. For example, the research team found that integrating data from three different systems (criminal, military, and humanitarian) reduced the time it took to determine a response to an event request from weeks to days [17].

When applying these tools to crimes falling under Chapter XIX of the Criminal Code of Ukraine, specific challenges arise: the need to correlate military logistics and organizational data with evidence of a gross violation of international humanitarian law; to ensure a standard of admissibility of evidence when working with large analytical systems; to guarantee the independence of the analysis from political or military pressure. These challenges require adapted procedures that take into account military specifics.

In practice, analytical systems also allow for modeling liability scenarios – for example, analyzing "who gave the order", "which units acted", "which logistical channels were used", "what consequences". This allows investigators to formulate chains of responsibility, which is key when prosecuting war crimes.

At the same time, the creation of integrated databases during military operations faces security and access problems: military zones, limited communications, the risk of cyberattacks, damage to data carriers – all this complicates the centralization of information. Therefore, the development of modular systems that can operate in conditions of partial availability and the use of backup transmission and storage channels is a critical prerequisite.

It should be noted that criminal analysis tools in a military context are a powerful tool for investigating war crimes under Chapter XIX of the Criminal Code of Ukraine, but their effectiveness depends on the correct integration of technical systems, procedures, personnel training and legal support. Without this, they can remain only a technological possibility, and not a real means of bringing to justice. Further development should focus on adapting analytical systems to the conditions of military operations, building integrated data and unifying application procedures.

8. Artificial intelligence in the process of investigating war crimes

In the context of investigating war crimes under Chapter XIX of the Criminal Code of Ukraine, the use of artificial intelligence (AI) systems is gaining strategic importance. In particular, machine learning algorithms open up possibilities for automatic recognition of persons, objects and signs of violence in large data sets – photos, videos, satellite images – that correlate with events falling under the definition of war crimes [18].

Such an application has several aspects. First, algorithms analyze metadata, frame images and video streams, identify specific individuals by facial features, cyber identifiers or forms of military equipment. This approach allows investigators to quickly establish, for example, who was in the area of shelling or destruction of civilian infrastructure. At the same time, this raises the question of the evidentiary admissibility of such materials in courts – it is necessary to provide evidence that the algorithm worked properly and did not contain significant errors. Second, automated sorting of large-scale evidence sets – videos, images, text messages – allows investigators to manage time and resources more effectively. The third key area is the detection of fake or altered digital evidence (deepfake-detection). In a military context, the use of disinformation and manipulated videos/screenshots is becoming a strategic issue, as such materials can serve as a “line of defense” against liability for war crimes. Machine learning systems successfully identify fake images, but the legal basis for their use is not yet fully formed [19]. Another important element is the combination of AI tools with traditional investigative procedures and international standards. For example, using AI to build chronologies of events, map damage and movements of military formations, and then compare this data with operational reports, testimonies and material traces creates a stronger

evidentiary chain. Domestic scientists emphasize that it is precisely such an integrated application of AI that contributes to the compliance of evidence with the requirements for confirming the composition of a war crime.

However, there are significant challenges. First of all, AI algorithms often act as a "black box": their decisions are difficult to explain, which poses risks to the admissibility of evidence in court. Such opacity undermines the trust in automated tools in the context of international criminal law [20]. In the case of war crimes investigations, this means the need to involve experts, document data on the training of models and ensure that the algorithms are auditable. When an AI system is applied to a war crimes case, the issue of preserving the integrity of the data and controlling the collection and processing procedure becomes critical. For example, the passage of digital evidence through algorithmic processing must be accompanied by metadata registration, change tracking and clear documentation of the results – so that they can be presented in court as reliable. Researchers emphasize that without such guarantees, the effectiveness of AI applications is significantly reduced and may be challenged in appeal procedures [21].

Therefore, the introduction of AI into the investigation of war crimes opens up significant opportunities: increasing the speed and depth of analysis, expanding the evidence base, highlighting hidden patterns. At the same time, it is not an "out-of-the-box" technological solution, but a complex integration of technology, procedures, legal support and personnel training. In the context of Chapter XIX of the Criminal Code of Ukraine, this means that investigative bodies and prosecutors must ensure that new technologies comply with the requirements of criminal law and international humanitarian law.

In the future, it is recommended to: (1) develop national standards for the use of AI systems in war crimes cases; (2) create training modules for investigators and prosecutors on the specifics of working with algorithms; (3) ensure independent examination of algorithmic solutions and openness of procedures. Only such an approach will allow transforming the potential of AI into a real tool for bringing to justice war crimes.

9. Prospects for creating joint databases of war crimes using IT technologies

One of the key trends in the modern development of criminal justice in Ukraine is the gradual digitalization of the processes of investigation and accounting of criminal offenses. In this context, the creation of joint databases of war crimes, provided for by Chapter XIX of the Criminal Code of Ukraine, is a strategically important direction for increasing the efficiency of pre-trial investigation, control over discipline and transparency of law enforcement in military formations.

Information and analytical systems capable of accumulating information on offenses committed by military personnel should provide a comprehensive approach to data collection, verification and analysis. This is about the possibility of integrating information from various sources – the Unified Register of Pre-Trial Investigations, military prosecutors' offices, military units, disciplinary commissions, etc. – into a single digital environment in compliance with cybersecurity and personal data protection requirements.

The use of IT solutions in the creation of such databases will allow for multidimensional criminal analysis (including temporal and spatial, behavioral and statistical), which will help identify systemic problems of military discipline and predict criminogenic trends in military groups. This is especially relevant in conditions of martial law, when the intensity of hostilities and the psychological burden on servicemen create additional risks of committing crimes, such as disobedience, desertion or violation of the statutory rules of relations between servicemen [22].

In addition, shared databases can become an effective tool for internal control over compliance with military discipline and prevention of recurrence of offenses. Systematized digital information will allow not only to document the facts of crimes, but also to analyze risk factors, service history of servicemen, and circumstances of disciplinary violations. This will facilitate the adoption of management decisions at the command level and the Ministry of Defense of Ukraine in order to strengthen law and order in military units [23].

It is important that such information systems be created on the principles of compatibility with existing state registers and taking into account international data processing standards. In particular, NATO's experience with unified information and analytical security systems (Defense Information Infrastructure) shows that sharing data in real time contributes to increasing the efficiency of military management and timely response to violations [24].

In the future, the creation of such databases has not only technical but also legal significance - it provides for the legislative definition of the status, procedure for functioning, the circle of users and access levels. This will allow to improve the quality of the investigation of war crimes, ensure the completeness of statistical accounting and create a basis for further analysis of criminogenic processes in the military sphere.

10. Conclusion

As a result of the study, it was established that the use of modern information technologies in the process of investigating war crimes is not only a technical, but also a systemic institutional and legal factor in increasing the effectiveness of criminal prosecution in wartime. The digitalization of evidence transforms traditional methods of forensics, opening up new opportunities for collecting, verifying and preserving evidentiary information, especially in conditions of active hostilities, when access to the scene of events is limited.

Digital technologies - photo, video recording, metadata analytics, OSINT tools, satellite monitoring systems - ensure increased objectivity, reliability and transparency of the evidentiary process. They create a comprehensive evidence base that allows establishing the temporal and spatial sequence of events and confirming the fact of committing a crime.

The key prerequisites for the effective use of information technologies are the regulatory consolidation of procedures for collecting, recording, verifying and storing digital evidence. Failure to comply with these requirements leads to the risk of losing the evidentiary value of materials obtained in the digital environment, and therefore to the complication of the judicial perspective of criminal proceedings. Therefore, the task of implementing international protocols of digital forensics into national legislation arises.

It is necessary to form a specialized infrastructure of digital forensics in the military justice system. This involves the creation of secure data exchange channels, mobile field laboratories for collecting digital evidence, as well as interagency platforms for coordination between investigators, prosecutors, experts and representatives of international missions. Such institutional mechanisms will ensure the unity of standards for investigating war crimes and strengthen international trust in the results of the investigation.

The use of open source technologies (OSINT) and satellite intelligence is a separate direction of development of forensic support for military investigations. These methods allow for the prompt detection and documentation of war crimes even in areas where physical access is impossible. At the same time, they require compliance with strict criteria for reliability, verification and preservation of the chain of evidence, which requires further regulatory detailing.

Technological modernization of investigative activities will be effective only if specialists are properly trained. Systematic training of investigators, prosecutors and forensic experts in methods of working with digital sources is necessary, covering issues of cybersecurity, data protection and international standards for verification of evidence.

Effective investigation of war crimes in modern conditions is possible only with a combination of three interdependent components: technical infrastructure, regulatory and procedural support and personnel competence. Their harmonization ensures the achievement of the goals of criminal justice - establishing the truth, bringing the guilty to justice and restoring justice even in wartime.

Modern information technologies are becoming an integral element of the legal mechanism for ensuring the military security of the state. Their effective use in the investigation of war crimes should be based on scientifically sound methodology, unified technical standards, interagency

coordination and continuous development of human resources. This is the strategic direction of the transformation of the Ukrainian military justice system in accordance with the principles of the rule of law, transparency and international accountability.

11. References

[1] O. M. Sarnavskyi, "Norms on the Criminal Liability of Military Personnel in the Criminal Law System of Ukraine," *Journal of the Kyiv University of Law*, no. 2, pp. 308–311, 2013.

[2] M. O. Yankovy, "Investigation of Criminal Offenses Committed by Military Personnel during an Armed Conflict: Statement of the Problem," *Academic Visions*, no. 18, 2023. Electronic resource. Accessed via: https://www.academy-vision.org/index.php/av/article/view/282

[3] Criminal Procedure Code of Ukraine, No. 4651-VI, 2012 (as amended). Electronic resource. Accessed via: https://www.wipo.int/wipolex/en/legislation/details/9021

[4] O. S. Kaplina, "Electronic Evidence in the Criminal Process of Ukraine: Theoretical and Applied Aspect," *Bulletin of Criminal Justice*, no. 4, pp. 47–53, 2021.

[5] M. I. Khavronyuk, "Digitalization of Criminal Justice in Ukraine under Martial Law," *Legal Bulletin of Ukraine*, no. 3, pp. 119–127, 2022.

[6] S. Dubberley, A. Koenig, and D. Murray, *Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation, and Accountability*, Oxford: Oxford University Press, 2020.

[7] S. Higgins, "Truth in a Digital Age: The Role of Open Source Investigations in International Criminal Justice," *Journal of International Criminal Justice*, vol. 19, no. 1, pp. 45–60, 2021.

[8] A. Smeulers, Perpetrators of Mass Atrocities: Theory, Typology and Comparison, London: Routledge, 2023.

[8] A. Koenig and L. Bittner, "Digital Evidence and the Future of International Criminal Law," *International Review of the Red Cross*, vol. 104, no. 919, pp. 65–78, 2022.

[9] M. G. Kolodyazhny, "Criminological Characteristics of Military Crimes in Ukraine," *Issues of Combating Crime: Collection of Scientific Works*, issue 26, pp. 109–117, Kharkiv: Pravo, 2013.

[10] E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, 3rd ed., Amsterdam: Academic Press, 2011. Electronic resource. Accessed via: https://www.sciencedirect.com/book/9780123742681/digital-evidence-and-computer-crime

[11] V. Khakhanovskyi and M. Hrebenkova, "Identification, Collection, and Investigation of Electronic Imagery as Sources of Evidence," *Law Journal of the National Academy of Internal Affairs*, vol. 12, no. 4, pp. 28–39, 2023.

[12] ISO/IEC 27037:2012, *Information Technology – Security Techniques – Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence*, Geneva: International Organization for Standardization, 2012.

[13] E. Higgins, *We Are Bellingcat: An Intelligence Agency for the People*, London: Bloomsbury Publishing, 2021.

[14] A. Bilous, I. Bodnenko, and S. Lokaziuk, *Open-Source Intelligence for War Crime Documentation*, Kyiv: CPITS, 2024.

[15] F. Millett et al., "Open-Source Intelligence, Digital Evidence and Accountability in Armed Conflict," *Journal of Human Rights Investigations*, 2023.

[16] V. Kovalchuk, S. Melnyk, and A. Sidorchuk, *Criminal Analytics Tools in the Ukrainian War Crime Investigations*, Kyiv: Institute for Strategic Data Studies, 2024.

[17] I. Petrov and O. Ivanenko, *Integrated War-Crime Databases: Challenges and Pathways in Active Conflict Zones*, Kharkiv: Center for Legal Informatics, 2023.

[18] V. Shepitko, M. Shepitko, K. Latysh, M. Kapustina, and E. Demidova, "Artificial Intelligence in Crime Counteraction: From Legal Regulation to Implementation," *Social and Legal Studies*, vol. 7, no. 1, pp. 135–144, 2024.

[19] B. Lorch, N. Scheler, and C. Riess, "Compliance Challenges in Forensic Image Analysis under the Artificial Intelligence Act," *arXiv*, 2022. Electronic resource.

[20] A. R. Greipl, "Data-Driven Learning Systems and the Commission of International Crimes," *Journal of International Criminal Justice*, vol. 21, no. 5, pp. 1097–1120, 2023.

[21] M. Beitler and E. T. Jensen, "Battlefield Artificial Intelligence and War Crimes Prosecutions," *Texas Tech Law Review*, vol. 56, pp. 689–724, 2024.

[22] V. Kulyk and A. Kyslyi, "Military Discipline and Criminal Liability in the Armed Forces of Ukraine: Legal and Organizational Aspects," *Baltic Journal of Law & Politics*, vol. 16, no. 2, pp. 233–249, 2023.

[23] O. Kostyuchenko and H. Ponomarenko, "Information Technologies in the Prevention of Military Crimes: Ukrainian Experience and NATO Standards," *Security and Defense Quarterly*, vol. 40, no. 1, pp. 55–70, 2022.

[24] NATO Communications and Information Agency (NCIA), *Defense Information Infrastructure: Lessons Learned and Future Development*, Brussels: NATO Press, 2021.