Pakistan Journal of Criminology
Vol. 16, No. 02, April—June 2024 (601-618)

Effectiveness of Forensic Computer Modeling for Predicting Wartime Crimes

Yurii Yelaiev[1], Ihor Fedchak[2], Volodymyr Senyk[3],
Dmytro Tymchyshyn[4] & Pavlo Nazarenko[5]

Abstract

This article emphasises the importance of computer models in forensics and their potential for predicting criminal activity and preventing offences in the context of military confrontation. The purpose of this paper is to determine the possibility of using computer models to analyse and predict criminal activity during military confrontation. The research employed the following methods: historical method of studying law, logical approach, qualitative method, method of analysis, and method of legal modelling. The study found that forensic modelling is mainly used at the pre-trial investigation or trial stage. The analysis of modern armed conflicts gives grounds to conclude about the high efficiency of computer modelling in preventing wartime crimes. The academic novelty is the obtained results of using computer modelling to prevent potential offences as opposed to its widespread use at the stage of pre-trial investigation. The research prospects include the possibility of the potential study of forensic computer modelling algorithms for accurate prediction of types of offences during the war.

Keywords: Computer modelling, forensics, armed conflict, criminal offence, international courts.

Introduction

In today's world, where military conflicts and crime have complex dynamics, it is important to have effective tools to predict possible offences during

[1] The author is a Lecturer of the Department of Organization of Pre-trial Investigation of Faculty №1 of Kryvyi Rih Educational & Scientific Institute, Donetsk State University of Internal Affairs, Ukraine. He can be reached at urrelaev@gmail.com
[2] The author is a Candidate of Legal Sciences, Associate Professor of the Department of Information and Analytical Support of Law Enforcement Agencies, Faculty 2, Lviv State University of Internal Affairs. He can be reached at fia_lv6h@i.ua
[3] The author is a Candidate of Technical Sciences, Associate Professor of the Department of Computational Mathematics and Programming, Institute of Applied Mathematics and Fundamental Sciences, Lviv Polytechnic National University, Ukraine. He can be reached at vol.vas.senyk@gmail.com
[4] The author is a Candidate of Law Sciences, Docent of the Department of Law and Humanities Open International University of Human Development "Ukraine" Ivano-Frankivsk Branch, Ukraine. He can be reached at andriy_tymch@ukr.net
[5] The author is a Candidate of Sciences in Law, Associate Professor of the Department of Criminal, Civil and International Law, National University "Zaporizhzhia Polytechnic", Ukraine. He can be reached at Pavelnazarenkoo67889@gmail.com

such events. Using computer models allows analysing and forecasting of various scenarios of the development of events based on collected data and statistics.

The current conditions for the development of forensic science identify important problems of forensic science that need to be addressed immediately. The most significant problem is the lack of methods that could help investigate and prevent new criminal offences (Shevchuk, 2021).

The importance of the chosen research issue is based on the fact that the correct forecasting of offences during a military conflict enables taking proactive measures to protect the population and property. This can significantly reduce the number of victims and the extent of damage, which is important from a humanitarian perspective. Furthermore, forensic computer modelling allows rational use of limited resources, directing them to where they are most needed to prevent offences and criminal activities during military conflict (Tymoshenko et al., 2022). Computer modelling aims to develop the existing methods of forensic science and adapt them to modern types of criminal offences in the context of war (Latysh & Demidova, 2021).

The relevance of the research is that the development of forensic computer modelling and data analysis provides new opportunities for effective forecasting of events in wartime. Using artificial intelligence, big data analysis, and other technologies can significantly improve the accuracy and effectiveness of forecasting. An additional argument for the study's relevance is that humanitarian crises often accompany military conflicts, and accurate forecasting of violations can help humanitarian aid organisations plan and respond more effectively. An innovative direction in the development of forensics is the development of protection against modern crime, including war crimes, and its implementation in forensic practice (Hunkha et al., 2022).

The current challenges and threats create a need for the development and implementation of innovative approaches in the forensic defence of war crimes, which determine the current trends in the development of legal science, in particular forensics, and focus on the problems of studying the use of digital technologies in the forensic investigation of war crimes in wartime and digitisation processes (Shevchuk, 2020b). Therefore, the current tasks of digital forensics are forensic modelling, search and analysis of digital traces, data analysis (including metadata) and collection of evidentiary information in the digital environment (Avdieieva, 2022).

Research objectives.

So, the aim of the study was to assess the effectiveness of forensic computer modelling in predicting wartime crimes. The aim involves the fulfilment of the following research objectives:

1. Analyse modern theoretical approaches to forensic computer modelling and their application in predicting offences during a military conflict.

2. Identify examples of successful application of forensic computer data to the main experiences of different countries and decisions of international courts.

3. Collect and analyse statistics on computer modelling in the context of wartime crimes.

4. Develop forecasting of crime reduction using forensic modelling.

Methodology

Research design.

The preparatory stage involved a comprehensive study, which included the analysis of statistics provided by the Office of the Prosecutor General of Ukraine regarding criminal offences in wartime. The Prosecutor General's Office provided information on crimes against the civilian population, violations of the rules of international humanitarian law, and crimes against the foundations of national security. A statistical research of the Kantar (2023) analytical group was studied regarding the attitude of Ukrainians to AI, including computer modelling in wartime. About 1,000 Ukrainians aged 18 to 55 were interviewed during a study conducted by the analysts. According to the survey results, it was established that 80% of the respondents belong to the youth aged 18 to 29, and 82% have a personal income of 10,000 hryvnias or more. Most respondents — 76% — understood the advantages of AI elements.

The experimental stage of the study included the analysis of survey results and their comparison with real situations in armed conflicts. Armed conflicts in Yugoslavia, Ukraine, and Georgia were analysed to understand the dynamics of crimes and apply forensic modelling to prevent them. The effectiveness of this method was determined by comparing the results of the analysis of armed conflicts with the results of the use of forensic modelling in wartime to prevent crimes. Its application enables taking into account contextual features and developing more effective strategies for managing the criminal situation in wartime.

The final stage involved concluding the effectiveness of using forensic computer modelling to combine forensic expertise with modern data processing and analysis technologies. It is used to analyse large volumes of data and identify connections and patterns that help make strategic decisions.

Methods

The research methodology includes a system of general scientific and sectoral legal methods. The use of the logical approach is determined by the need to define the conceptual and categorical framework, including "forensic computer modelling" and "military conflict". This method was also applied to understand the methods and technologies used to analyse data and predict possible offences in the context of armed conflicts.

The historical method of studying law was applied to review historical examples of military conflicts and the legal system's reaction to them. The methods and tools used to predict offences during these conflicts were determined. The purpose of applying the comparative law method to study the effectiveness of forensic computer modelling was to clarify different legal approaches and practices in different jurisdictions regarding using such technologies in wartime. In the case of forensic computer modelling in the context of armed conflict, this method made it possible to study various approaches to using computer technologies in criminal justice and investigating crimes during conflict situations.

Applying the logical semantic method aimed to examine the logical connections between various aspects of forensic computer modelling and armed conflict. This includes the relationship between digital footprint detection, data analysis and real-time decision-making during conflict. A qualitative method was used to analyse data on criminal offences and compare them with facts about various aspects of using forensic computer simulations in armed conflicts. The purpose of applying this method is to analyse the decisions of international courts and statistics of law enforcement agencies.

Sample

The selection of Yugoslavia, Kosovo, Georgia, and Ukraine to analyse the use of computer simulations in armed conflicts has several sound reasons. These countries represent a variety of armed conflicts that occurred at different times and have different causes and characteristics. Including countries with different contexts allows for a wider range of data for analysis. Yugoslavia and Kosovo in the mid-1990's became the scene of intense military operations and inter-ethnic conflicts. Georgia and Ukraine have also experienced armed conflicts, such as the war in Transnistria, Abkhazia, South Ossetia (for Georgia) and the Russian-Ukrainian war (since 2014). Events in Yugoslavia, Kosovo, Georgia, and Ukraine reflect modern challenges in international relations, conflicts, and security. Research on computer simulations in these conflicts can help develop more effective international cooperation and peacekeeping strategies. Armed conflicts on the territory of these countries are relevant and interesting for research, as they

have a great impact on regional and world politics, as well as on the socio-economic situation in the countries.

Literature review

Efforts to combat criminal activities are indispensable for societal stability and advancement. Law enforcement entities endeavour to effectively control offenders and criminal organisations, considering the unique characteristics of illicit behaviour (Tyagi, 2018).

Technologies based on artificial intelligence (AI), including computer simulations, have significantly expanded their capabilities and become more accessible and widely used in recent years (Caldwell et al., 2020). One of the first modern political and legal examples of computer modelling is the investigation of the explosion opposite St. George Street in downtown Beirut on February 14, 2005. This is the first time this technology has been used in an international criminal tribunal (Freeman, 2018).

Over the past decade, international criminologists have increasingly used digital technologies to detect, analyse, and prevent crimes (Yurchyshyn, 2021). Initially, the adoption of novel technologies was perceived as ineffectual and untested. Nonetheless, with time, methodologies were devised that facilitated the amalgamation of vast online datasets with digital techniques, yielding crucial insights for investigating diverse crimes globally.

Computer modelling certainly cannot completely replace traditional evidence collection methods, but it must be considered in conjunction with other evidence. Therefore, it has many uses, including applications in criminal investigations, transitional justice strategies, truth, reconciliation efforts, etc. (D'Alessandra & Sutherland, 2021).

Proficiency in information processing and database creation is vital for simulating crimes using computers. Social networks serve as invaluable resources for gathering considerable information during military operations, including testimonies from victims and witnesses. However, these platforms have limitations in accurately portraying certain events and evaluating their repercussions (Remkes, 2019).

Demonstrative evidence, which includes charts, maps, drawings, graphs, animations, simulations, and models, is information that helps judges to better understand the evidence rather than the evidence itself. The characteristics of contemporary warfare have heightened the significance of intellectual elements in military operations (Hrytsai, 2023). In crimes associated with armed conflicts, this presents opportunities for leveraging novel forms of data that may be admissible as evidence in legal proceedings (Latysh, 2022).

Image recognition technology, such as improvised explosive devices, is used during armed conflicts to predict potential threats and risks (Shulha et al., 2021). This technology is used in war crimes investigations to identify objects after an attack, such as fragments of an explosive device. The same algorithms used to distinguish civilians from combatants before an attack can be applied to identify these differences in causality after an attack (Yang et al., 2019).

The same technologies can also be used for war prevention, humanitarian response to war, and investigating alleged war crimes. Shah et al. (2018) stated that the accuracy of crime prediction, according to their research, is 90% for less complex data sets, but the accuracy drops to 60% for complex data sets.

Using simulations utilising technologies like social networks, cloud computing, mobile devices, data compression, encryption, and diverse forms of malware by law enforcement agencies is contentious due to their potential intricacy and the challenges they pose in investigations (Thakar et al., 2021). Four "new technologies" with features of computer modelling are currently used in forensics:

- Geospatial Intelligence and Remote Sensing (GEOINT);
- Open-Source Intelligence (OSINT);
- Financial Intelligence (FININT);
- Documentation technologies —from simple cameras to specialised software, such as the innovative eyeWitness to Atrocities programme-enable recording photos and videos and adding relevant metadata to prove their authenticity in court (Hunkha et al., 2022).

The full-scale aggression of the Russian Federation also affected the development of forensics. It is important to note that the key for the courts of Ukraine is to establish a correlation between the actions of the aggressor nation, including personnel from the Russian armed forces, and the resulting outcomes, notably the inflicted harm (Shevchuk et al., 2022). For this purpose, it is necessary to intensify the development of technologies based on current forensic knowledge, with intensive use of digital technologies, including artificial intelligence and computer modelling (Shepitko et al., 2021).

The literature review makes it clear that many studies confirm the necessity of using computer technologies in forensics in wartime. This is determined by the increasing complexity of crimes and the need for highly accurate tools for their detection and countermeasures.

Results

The concept of computer modelling in the field of forensics is relatively new. However, the possibility of developing electronic forensics as one of the main elements of the crime prevention system was enshrined in international legal acts.

Analysis of current theoretical approaches to forensic computer modelling and their application in predicting offences in wartime

Article 33 of the Geneva Convention for the Protection of Civilian Persons in the Event of War defines measures to be taken to prevent violations of conventions and other international provisions during war (ICRC, n.d.). Computer simulations can be used to develop intervention strategies and monitor military conflicts to prevent crimes. Article 25 states that the parties to the conflict must avoid taking any action that may result in disproportionate risks to the civilian population. Computer simulations can be used to assess risks and determine measures to reduce them.

Regarding the Council of Europe, the Budapest Convention on Cybercrime contains provisions on combating cybercrime, including computer simulations to predict and prevent cybercrime. It provides a framework for international cooperation in this area. The General Data Protection Regulation (GDPR) sets out rules for personal data processing, including data that can be used in forensic computer models. It significantly impacts the work of law enforcement agencies and companies involved in developing and using such models in the EU (European Union, 2016).

The forensic computer simulations developed by Actlyzer study (Fujitsu, 2020) demonstrated that such basic actions, such as walking and stopping, to more complex movements can be almost definitely recognised. In 2020, the United Nations prepared the Berkeley Protocol on Digital Open Source Investigations. This document has become an important tool in using open sources of digital information while investigating violations of international criminal law and international humanitarian law (IHL) (United Nations, 2020).

The doctrinal approach gives grounds to conclude that forensic computer simulations have international legal regulation, but it needs to be detailed in terms of its potential ways of application. This method is used to prevent war crimes, humanitarian crimes and facilitate the investigation of alleged war crimes.

Forensic computer simulations based on the main experiences of different countries and decisions of international courts

The historical method of studying law was used to determine that computer simulations were used during armed conflicts in Yugoslavia, Georgia, and Kosovo. One of the practical examples of the use of forensic modelling in the war in Yugoslavia is the work of the International Criminal Tribunal for the former Yugoslavia (ICTY) (Prosecutor v. Callixte Mbarushimana, 2011). The ICTY used forensic modelling to analyse crime scenarios and crime scenes. This made it possible to recreate events based on evidence and testimony, carry out simulations of possible options, and use this data in legal proceedings to clarify the facts and establish the guilt of guilty persons. In the ICTY Krstić and Srebrenica cases, visual digital evidence was used in international criminal courts and tribunals and had strong roots in ICTY case law. The International Criminal Court relies heavily on this legacy (Cases) (Prosecutor v. Krstić, Case No. IT-98-33-T, 2001).

In 2001, the war in Kosovo posed a serious threat to the local population and international forces. Computer simulations made it possible to analyse geographic data, social, and ethnic factors contributing to conflicts. Areas of potential armed conflict were identified, and resources were directed to conflict prevention. This helped to quickly react to possible threats and prevent them.

During the 2008 conflict between Russia and Georgia, there were several situations where forensic modelling was used to investigate the events and analyse the circumstances of the conflict. One of the examples is the investigation into the circumstances of the bombing of the city of Gori during the conflict. This included analysing the location of military units, the routes of military operations, and the timing of missile launches. Forensic modelling could help to identify possible sources of fire that led to the bombing of the city.

The method of comparative law was used to determine the progress of the development of forensic modelling. Progress in forensic modelling has been found since the war in Yugoslavia to the Russian-Georgian war and the Russian-Ukrainian wars. In particular, it was established that this method enables determining the schemes and locations of the armed forces of different states, which aims to prevent the commission of offences. This method allowed for the analysis and comparison of legal norms, strategies, and practices related to forensic modelling in different countries and jurisdictions.

One example of successful crime reduction using wartime forensic modelling is predicting criminal activity as part of the Iraq wartime crime-fighting effort. In 2007, PredPol was developed in the United States, based on analysing

criminal data and predicting the places and times of potential crimes. This programme was first used in Los Angeles to fight crime, but then it was successfully used in a military environment. During the war in Iraq, US military and criminal analysts used data from various sources, such as reports from military units, surveillance of people's movements, signals from intelligence sources, etc., to analyse crime and predict where and when it might increase. The result of this analysis was the establishment of certain crime patterns, such as places of frequent attacks on patrols or other forms of crime. One of the measures that was taken was increased patrolling and response in these specific areas and at particular times. We believe that the successful experience of using forensic modelling during the war in Iraq is an example of the potential development of other models of forensic modelling. This will reduce the crime risk and provide greater security for the local population and military units. Forensic modelling made it possible to optimise the allocation of resources and effectively use them to prevent crime in wartime.

Data and statistics of the use of computer modelling in the context of crimes during military conflicts.

Forensic computer simulation is a useful tool for crime prevention in wartime in Ukraine. According to the Prosecutor General's Office of Ukraine, criminal proceedings were registered and initiated in Ukraine for the number of crimes indicated in Figure 1 as of the beginning of 2023 (Armyinform, 2022). The Figure 1 shows that the largest number of criminal proceedings are war crimes since the full-scale Russian – Ukrainian war. Given the large number of proceedings, forensic modelling can speed up the pre-trial investigation procedure by quickly processing large data volumes.

Analytical software for processing information on the movement of troops and intelligence data is used during the conflict in eastern Ukraine. For the trial of war crimes, the key factor will be the establishment of a causal relationship between the actions of Russia, its military leadership, and the damage caused.

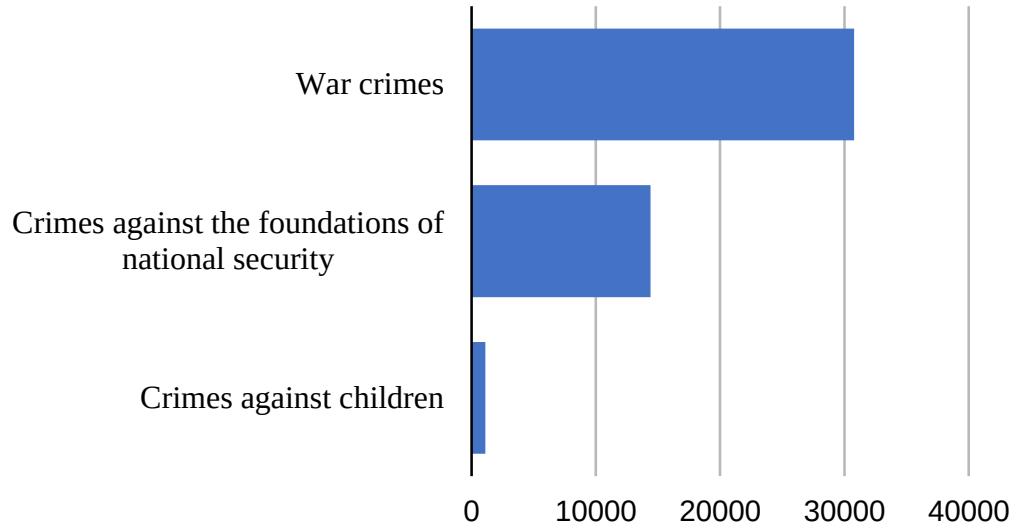

Figure 1. Registered criminal proceedings in connection with the aggression of the Russian Federation according to the Prosecutor General's Office as of the beginning of 2023.

Forensic computer simulations were used in the case of the downing of MH17 by Russian troops on the territory of Ukraine. In particular, on November 17, 2022, The Hague District Court issued a verdict in the MH17 criminal case (de Rechtspraak, 2022). In the course of the trial, the court examined, among other things, the evidence obtained through electronic modelling and the video recording of the movement of the Buk air defence system was examined. In the verdict, the court describes many intercepted conversations, as well as photo and video materials, using them as the basis for making several conclusions regarding the actions of the accused and their role. The court noted that electronic and natural tests were also conducted with the Buk missile.

One of the modern examples of an effective computer simulation and artificial intelligence system during a military conflict is ClearView AI. At the beginning of the full-scale Russian invasion of Ukraine, this system analysed almost 2 billion photos from social networks for potential verification of saboteurs and war criminals.

In 2023, the analytical company Kantar conducted a sociological survey on the attitude of Ukrainians to the development of artificial intelligence, including computer simulation. The interviewees were able to answer the question: which spheres of social life most need the development of computer simulation today (Kantar, 2023).

Statistical results demonstrate that (Figure 2), despite the third year of full-scale aggression by the Russian Federation, Ukrainians are not fully aware of the importance of modern forensic methods. This indicates that the development of computer simulation in wartime in Ukraine is currently at the primary stage only. We believe that the reason is also that Ukraine, being in a state of war, suffers from a shortage of resources for the development and implementation of current forensic methods. So, in the context of military conflict, computer simulation can be applied in several areas of forensic examination, as shown in Figure 3.

Given the information presented in the figure above, the means of digital forensics represent a certain theoretical and practical interest. Computer simulation helps in the prevention of war crimes and contributes to the inevitability of punishing war criminals.

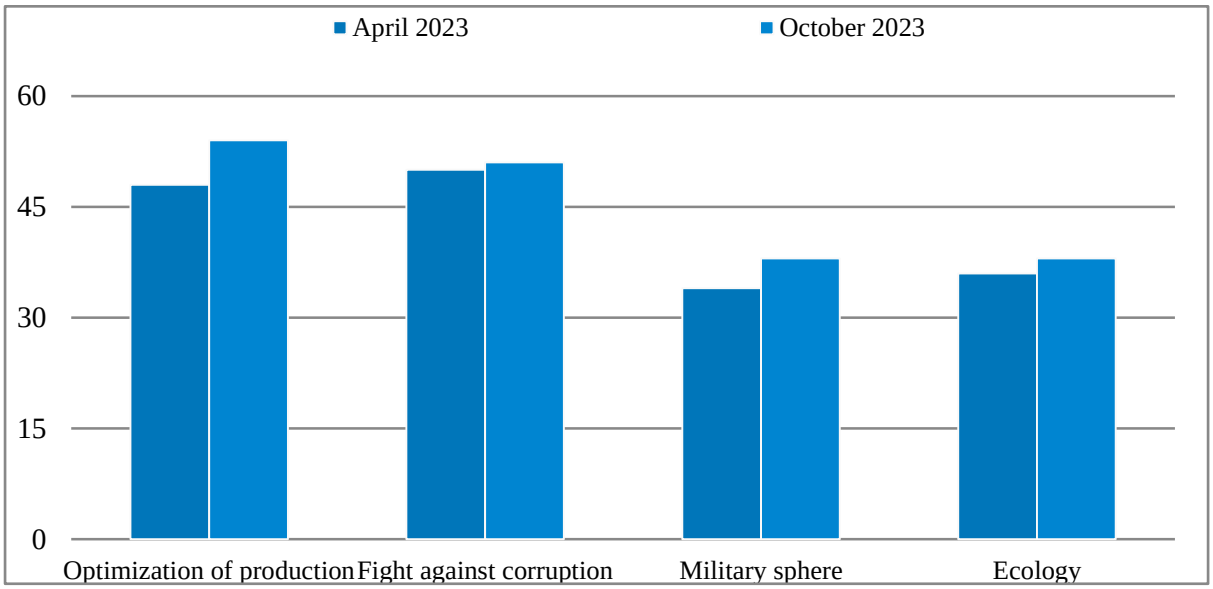

Figure 2. The potential of using AI, computer simulation in Ukraine

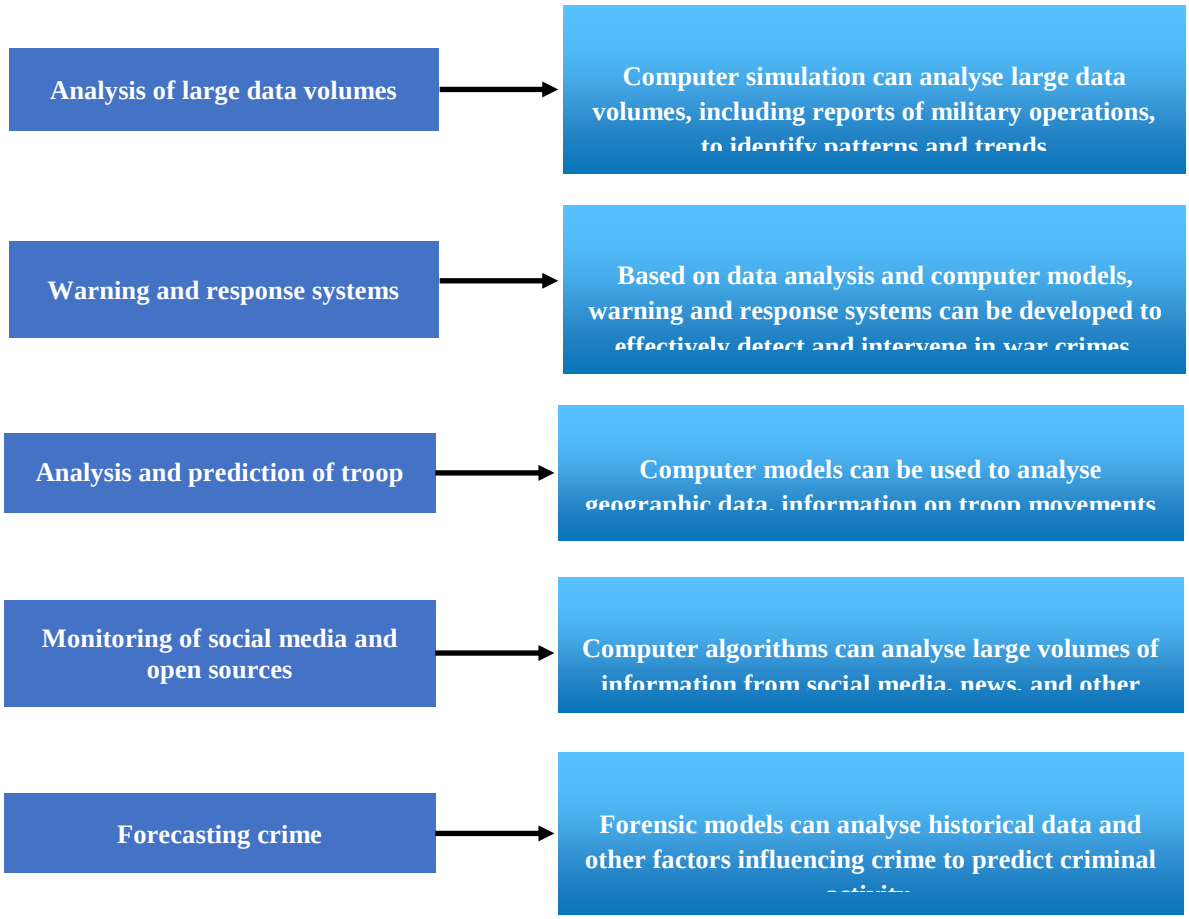

Figure 3. Schematic representation of the fields of use of forensic simulation in forensics in the context of armed conflict.

Forecasting crime reduction through forensic modelling

With the help of forensic modelling, it is assumed that implementing appropriate strategies and measures based on data analysis on criminal offences can lead to a decrease in the number of offences in a defined territory or a specific social group. This forecast is based on the analysis of historical data, taking into account social and economic factors that affect the criminal situation and using modern data analysis methods. It is expected that using such an approach will enable identifying and solving vulnerable issues in the field of offences, contributing to stabilising the situation and reducing the risk of committing crimes.

Forensic modelling can be used to analyse various aspects of a conflict, such as the distribution of military forces, local population dynamics, geographical features of the territory, ethnic and socio-economic factors.

Discussion

Computer modelling can help identify potential crime hotspots by predicting places and times where crimes are more likely to occur in armed conflict. Tyagi (2018) concluded that the main goal of developing forensics, including computer modelling, is the need for stability and development of society. In our opinion, given the political instability in the world, computer models and other electronic elements of forensic development enable identifying places where crimes are most likely to occur in wartime, helping law enforcement agencies to direct their resources to the most critical areas.

D'Alessandra and Sutherland (2020) rightly observe that computer modelling cannot completely replace the entire evidence base. We agree with this conclusion based on the decision of the International Criminal Court regarding the downing of MH17. It should be noted that computer modelling is an important additional tool in investigating criminal cases and administering justice. For example, computer models can help identify patterns and analyse large data volumes, allowing more effective detection of suspicious individuals or forecasting crime trends. Such a comprehensive approach ensures more objective and effective results in the consideration of criminal cases, as well as justice.

Considering the issue of the application of forensic computer modelling, including the analysis of videos and photos from social networks, we believe that Professor Yang et al. (2019) have significantly narrowed their conclusions regarding the modelling scope. The Professor believes that in times of war, image recognition technology is mainly used to predict potential threats and risks, such as improvised explosive devices, and to identify objects after an attack, such as fragments of an explosive device. We hold that the field of application of the technology is much wider; in particular, it enables the analysis and removal of photos of persons who could potentially be involved in sabotage or other criminal offences against the foundations of national security.

Remkes (2019) rightly states that the role of social networks is extremely high in using computer simulation to prevent criminal offences. Moreover, computer simulation enables the prediction of situations and the effective determination of strategies for preventing criminal offences. For example, analytical models can consider various factors, such as geographic location, demographics, criminal network structure, etc., to predict the locations and times of possible offences.

The importance of computer simulation in forensics is significant for analysing large volumes of information for crime prevention. Crime prevention should be a priority in view of the unstable political and legal situation in Europe as a result of the Russian Federation's aggression against Ukraine. We concur with Shevchuk's (2020a) perspective on the significance of determining a causal connection between the actions of the aggressor and the potential for preventing criminal offences.

Conclusions

The obtained research results are relevant because of the growing complexity of current military conflicts, which are characterised by advanced technologies. These challenges are related to developing tools for conflict analysis and forecasting. The analysis showed that forensic computer simulation has significant potential in predicting, detecting, and preventing war crimes. It enables the analysis of large data volumes and the identification of trends, which helps develop effective strategies to combat crime.

It is important to consider forensic computer simulation as part of an integrated crisis and conflict management system to achieve the goals of combating crime in wartime. Further research in this area could focus on developing methods to integrate various data sources, such as satellite imagery and social media, to obtain a complete picture of the situation. The work on improving forecasting systems can be done, including developing new models and approaches for more accurate forecasting of risks and events.

Recommendations:

- Continue the development of forensic modelling methods and improve data analysis algorithms, develop new mathematical models, and use advanced machine learning methods to improve the accuracy of predictions.
- Development of new forecasting models that consider the specifics of a military conflict, such as the dynamics of hostilities, strategic and tactical moments, local population dynamics, etc.
- Studying the effectiveness of using the results of forensic modelling in the strategic planning of actions in the conditions of a military conflict, including the development of optimal strategies for crime prevention and security.
- Exploring the possibilities of an integrated approach to the use of forensic computer simulation together with other methods of collecting and analysing information, such as intelligence, analytics, and expert evaluations, to obtain a complete understanding of the situation and develop comprehensive crime prevention strategies.

References

Armyinform. (2022). 68,019 crimes were committed during the Russian invasion, 460 children were killed. Retrieved from https://armyinform.com.ua/2023

Avdieieva, G. K. (2022). Problems of using digital forensics tools in the investigation of war crimes. In *The Use of Digital Information in the Investigation of Criminal Offences. Law* (pp.10-13). Kharkiv. Retrieved from https://dspace.nlu.edu.ua//jspui/handle/123456789/19547

Caldwell, M., Andrews, J. T. A., Tanay, T., & Griffin, L. D. (2020). AI-enabled future crime. *Crime Science*, 9, 14. https://doi.org/10.1186/s40163-020-00123-8

D'Alessandra, F., & Sutherland, K. (2021). The promise and challenges of new actors and new technologies in international justice. *Journal of International Criminal Justice*, *19*(1), 9-34. https://doi.org/10.1093/jicj/mqab034

de Rechtspraak. (2022). The District Court of The Hague has delivered the judgment in the MH17 criminal case at Schiphol Judicial Complex (JCS). Retrieved from https://www.courtmh17.com/en/about-the-case/

European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj

Freeman, L. (2018). Digital evidence and war crimes prosecutions: The impact of digital technologies on international criminal investigations and trials. *Fordham International Law Journal*, *41*(2), 283-336. Retrieved from https://ir.lawnet.fordham.edu

Fujitsu. (2020). Actlyzer – AI innovation unlocks behavioural analysis (Transforming AI behavior analysis accessibility). Retrieved from https://www.fujitsu.com/global/about/research/ article/202008-actlyzer.html

Hrytsai, S. (2023). Digital innovations in the legal mechanism of copyright authentication (Practical aspect): Can a non-functioning token be a guarantor of intellectual property? (NFT on the Example of Ukraine). *NTUT Journal of Intellectual Property Law and Management, 12*(2), 48–69. Retrieved from http://perspectives.pp.ua/index.php/nts/article/download/9383/9436/9437

Hunkha, R., Arrabal, C. T., Dantas, M. M., & Bassanelli, H. R. (2022). Laser scanner and drone photogrammetry: A statistical comparison between 3-dimensional models and its impacts on outdoor crime scene registration. *Forensic Science International*, *330*, 111100. https://doi.org/10.1016/j.forsciint.2021.111100

ICRC. (n.d.). Convention (IV) relative to the Protection of Civilian Persons in Time of War. Geneva, 12 August 1949. Retrieved from https://ihl-databases.icrc.org/en/ihl-treaties/gciv-1949

Kantar. (2023). A study on the attitude of Ukrainians towards artificial intelligence. The findings show a generally positive perception of the technology. Retrieved from https://www.kantar.com/ua/inspiration/consumers/ai-in-ukraine

Latysh, K. V, & Demidova, Y. E. (2021). Corruption offences in medications circulation: investigation problems. *Wiadomosci Lekarskie*, 7474(11), 2896-2900. Retrieved from https://pubmed.ncbi.nlm.nih.gov/35029552/

Latysh, K. V. (2022). Digital forensics during the war in Ukraine: Possibilities of using specialised knowledge in the field of information technology. *Kriminalistika ir Teismo Ekspertologija: Mokslas, Praktika*, 18, 31-37. Retrieved from https://cris.mruni.eu/server/api/core/bitstreams/a1f4cc9c-d2a8-4150-884c-4cfd267a92af/content

Prosecutor v. Callixte Mbarushimana. (2011). International Criminal Tribunal for the Former Yugoslavia. Retrieved from https://www.asser.nl/

Prosecutor v. Krstić, Case No. IT-98-33-T (2001). International Criminal Tribunal for the Former Yugoslavia. Retrieved from https://www.icty.org/x/cases/krstic/acjug/en

Remkes, M. (2019). Frontstage and backstage in Argentina's transitional justice drama: The Nietas' reconstruction of identity on social media. *International Journal of Transitional Justice*, 13(2), 349-367. https://doi.org/10.1093/ijtj/ijz008

Shah, M., Idrees, H., & Surette, R. (2018) Enhancing camera surveillance using computer vision: a research note. *An International Journal of Police Strategies and Management*, *41*(2), 292-307. https://doi.org/10.1108/PIJPSM-11-2016-0158

Shepitko, V., Konovalova, V. O., Shevchuk, V. M., Avdeeva, G. K., Getman, G. M., Pavlyuk, N. V., Yaremchuk, V. O., Sokolenko, M. O., Hryhorenko, A. O. (2021). Scientific and technical support of investigative activities in the context of an adversarial criminal procedure. *Issues of Crime Prevention*, *42*(42), 92-102. http://dx.doi.org/10.31359/2079-6242-2021-42-92

Shevchuk, V. (2020a). Forensic innovation: research prospects. *Theory and Practice of Forensic Examinations and Criminalistics: Collection of Scientific Papers, 22*, 20-40. https://doi.org/10.32353/khrife.2.2020.02

Shevchuk, V. (2020b). Problems of criminalistic support of the practice of the International Criminal Court in Ukraine. *Collection of Scientific Papers ΛΌГОΣ, 4*, 14-19. https://doi.org/10.36074/09.10.2020.v4.03

Shevchuk, V. (2021). Modern state and innovative directions of research of criminalistic technique. *InterConf, 46*, 221-233. https://doi.org/10.51582/interconf.19-20.03.2021.021.

Shevchuk, V., Vapniarchuk, V., Borysenko, I., Zatenatsky, D., & Semenogov, V. (2022). Criminalistic methodics of crime investigation: Current problems and promising research areas. *Revista Juridica Portucalense, 32*, 320-341. https://doi.org/10.34625/issn.2183-2705(32)2022.ic-14

Shulha, M. G, Mazur, A. V, & Georgiievskyi, I. V. (2021). Impact of epidemiological situation on respect for human rights and freedoms: informational aspect. *Wiadomosci Lekarskie, 74*, 2992-2998. Retrieved from https://pubmed.ncbi.nlm.nih.gov/35029568/

Thakar, A., Kumar, K., & Patel, B. (2021). Next generation digital forensic investigation model. *Journal of Physics: Conference Series*, 1767. http://dx.doi.org/10.1088/1742-6596/1767/1/012054

Tyagi, D. (2018). An approach to crime data analysis: A systematic review. *International Journal of Engineering Technologies and Management Research,* 5(2), 67-74. https://doi.org/10.29121/ijetmr.v5.i2.2018.615

Tymoshenko, Y. P., Kozachenko, O. I., Kyslenko, D. P., Horodetska, M. S., Chubata, M. V., & Barhan, S. S. (2022). Latest technologies in criminal investigation (testing of foreign practices in Ukraine). *Amazonia Investiga, 11*(51), 149-160. https://doi.org/10.34069/AI/2022.51.03.14

United Nations. (2020). Berkeley Protocol on Digital Open Source Investigations A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law. Retrieved from https://www.ohchr.org/

Yang, Z., Yu, W., Liang, P., Guo, H., Xia, L., Zhang, F., Ma, Y., & Ma, J. (2019). Deep transfer learning for military object recognition under small training set condition. *Neural Computing and Applications, 31*, 6469-6478. https://doi.org/10.1007/s00521-018-3468-3

Yurchyshyn, V. D. (2021). Forensic examination in the activities of the European Court of Human Rights: issues of theory and practice. *Law and Society, 2*, 240-245. Retrieved from http://www.pravoisuspilstvo.org.ua/archive/2021/2_2021/35.pdf