Lex Humana, v. 16, n. 1, 2024, ISSN 2175-0947

EFFECTIVENESS OF THE METHOD OF FORENSIC COMPUTER SIMULATION OF OFFENCES IN THE CONTEXT OF MILITARY OPERATIONS

EFICÁCIA DO MÉTODO DE SIMULAÇÃO COMPUTADORIZADA FORENSE DE OFENSAS NO CONTEXTO DE OPERAÇÕES MILITARES

NATALIIA AKHTYRSKA
Educational and Scientific Institute of Law, Taras Shevchenko National University of Kyiv, Ukraine
akhtyrrska@gmail.com

OLENA KOSTIUCHENKO
Educational and Scientific Institute of Law, Taras Shevchenko National University of Kyiv, Ukraine
helen.hrytsanchuk@gmail.com

ANNA VYNOHRADOVA
Educational and Scientific Institute of Law, Taras Shevchenko National University of Kyiv, Ukraine
g00dnot@ukr.net

TETIANA PAVLYSH
Donetsk State University of Internal Affairs, Ukraine
21tanyagrig12@ukr.net

SERHII BARHAN
Kryvyi Rih Educational and Scientific Institute, Donetsk State University of Internal Affairs, Ukraine
sergigan@gmail.com

Received: 15 Aug 2023
Accepted: 27 Nov 2023
Published: 10 Dec 2023

Corresponding author:
helen.hrytsanchuk@gmail.com

Abstract: Military operations cause various violations in the state security system, including an increased criminal activity. This requires improved and innovative response to offences and crimes, which include forensic computer simulation of offences. The aim of this work is to determine an approach to the development of a forensic computer model of offences in the context of military operations and to assess its potential advantages. The research involved the method of statistical observation, the rating method, the analysis of risks and potential failures using the FMEA model. The conducted research revealed an increased crime rate in Ukraine after the full-scale invasion. The increased number of particularly serious crimes by almost 9 times requires special attention. This gave grounds to propose the directions of application of the method of forensic computer simulation of offences — forecasting and analysis of crimes, geo-informational simulation, etc. An algorithm for the development of a forensic computer model for predicting terrorist acts in the context of a military conflict is proposed. It is noted that the effectiveness of this model depends on the correct identification and assessment of possible risks for the security system, which is proposed to be carried out using the FMEA model. The application of the FMEA model for predicting terrorist acts is the novelty of the study.

Keywords: Forensic Computer Simulation. Offence. Crime. Military Operations. Criminal Activity. Crime Rate. FMEA Model. Risk Prediction.

Resumo: As operações militares causam diversas violações no sistema de segurança do Estado, incluindo um aumento da atividade criminosa. Isto exige respostas melhoradas e inovadoras a infracções e crimes, que incluem a simulação computacional forense de infracções. O objetivo deste trabalho é determinar uma abordagem para o desenvolvimento de um modelo computacional forense de crimes no contexto de operações militares e avaliar as suas potenciais vantagens. A pesquisa envolveu o método de observação estatística, o método de rating, a análise de riscos e potenciais falhas utilizando o modelo FMEA. A investigação realizada revelou um aumento da taxa de criminalidade na Ucrânia após a invasão em grande escala. O aumento de quase nove vezes no número de crimes particularmente graves exige atenção especial. Isto deu motivos para propor as direções de aplicação do método de simulação computacional forense de crimes - previsão e análise de crimes, simulação geoinformacional, etc. Um algoritmo para o desenvolvimento de um modelo computacional forense para previsão de atos terroristas no contexto de um conflito militar é proposto.

Nota-se que a eficácia deste modelo depende da correta identificação e avaliação de possíveis riscos para o sistema de segurança, o que se propõe a ser realizado através do modelo FMEA. A aplicação do modelo FMEA para previsão de atos terroristas é a novidade do estudo.

Palavras-chave: Simulação Computacional Forense. Ofensa. Crime. Operações Militares. Atividade Criminal. Taxa de Crime. Modelo FMEA. Previsão de Risco.

1. Introduction

Military operations are a big challenge for the state, society, law enforcement agencies and the security system. War creates specific conditions in which crime and criminal activity can increase significantly leading to increased threats to the population and public order (Daly et al., 2020; Rawtani et al., 2022; Gostin and Rubenstein, 2022). This determines the relevance of studying the possibilities of modern information technologies (Ozkan, 2019; Milivojevic and Radulski, 2020; Ho et al., 2022) and analytical tools (Ren et al., 2019; Xu et al., 2020; Babuta and Oswald, 2020) to prevent and combat potential threats.

Forensic computer simulation of offences (Al-Dhaqm et al., 2020; Hoang et al., 2021; Kumar et al., 2022) can be effective in analysing, predicting and responding to crimes and offences in the context of military operations. It combines modern computer technologies and forensics methods, enabling law enforcement agencies and researchers to study crime patterns in the context of military operations. This method is useful for analysing and predicting risks and possible threats, and can offer measures and strategies to combat crime in critical conditions.

The example of Ukraine can be used to understand the destruction that war causes for the population, infrastructure, state, and the world as a whole (Ben Hassen and El Bilali, 2022; Boubaker et al., 2022; Mbah and Wasum, 2022). Moreover, it is a trigger for the activation of various criminal schemes, terrorist activities, and the spread of other crimes. This causes new challenges for the country's law enforcement agencies and the military. These challenges can be addressed through the improvement of the security system, which includes the prediction, analysis and assessment of probable risks and threats (Jin et al., 2020; Kolla, 2022; Prathap, 2022). This is where the method of forensic computer simulation of offences can be used as an effective tool for forecasting and developing ways to combat the spread of crime.

The aim of this article is to determine an approach to the development of a forensic computer model of offences in the context of military operations and to assess its potential advantages. The aim involved the fulfilment of the following research objectives:

- Study the crime rate in Ukraine during the war in order to assess criminal activity;

- Describe the areas of application and effectiveness of forensic computer models of offences in the context of military operations;

- Create an algorithm for the development of a forensic computer model for predicting terrorist acts in the context of a military conflict;

- Determine the appropriateness and advantages of using the FMEA model to assess the risks of terrorist attacks in the context of military operations.

2. Literature Review

The use of the latest information technologies in criminology is a promising direction for the development of this field, which is confirmed by numerous relevant studies. Studying the peculiarities of the application of innovative technologies in forensics, Sokurenko (2022) determines promising directions for the development of this field. The researcher notes that innovative technologies can not only optimize and simplify the drafting of documents and systematize the legal framework, but also have applications in the practice of investigating crimes. The researcher emphasizes that the key problem at the current stage is the lack of appropriate digital skills among forensic specialists.

Podobnyi and Slatvinska (2021) list the main tasks of informatization of law enforcement activities. The researchers come to the conclusion that the current system of combating crime in Ukraine is ineffective and cumbersome. This requires law enforcement agencies to significantly increase the efficiency of information provision with the use of innovative technologies. Cyber security is the main focus in the study.

In a number of studies, digital forensics is considered separately from forensics in general as a field related to countering cybercrime. In this regard, Casey (2019) points to the complexity of solving the problem of weak integration between forensics and digital forensics. The researcher notes the increase in the complexity of investigations because of the increasing volume of digital traces, which leads to a decreasing understanding of cybercrimes. This can result in imprisoning innocent people or giving criminals the freedom to commit new crimes.

Jarrett and Choo (2021) study the impact of specific technologies — automation and artificial intelligence — on the development of digital forensics. The researchers identify the following consequences for digital forensics: cost reduction, increased effectiveness and efficiency of forensic investigations, increased accuracy of information processing, etc. Based on the conducted literature review, the researchers provide a number of recommendations for increasing the efficiency of further

development. Dasaklis et al. (2021) study the possibilities of using another innovative technology in digital forensics. The researchers review and classify available blockchain-based digital forensic tools, emphasizing its advantages over more commonly used methods.

Jafari and Satti (2015) thoroughly compare the most used digital forensics process models: NIJ, DOJ, DRFWS, IDIP, EIDIP, Abstract Model and SRDFIM Model. The researchers describe the steps of implementing these models and compare them according to the individual stages and other criteria.

Some studies deal with the use of digital technologies not only for the detection of cybercrimes, but also for the investigation of ordinary offences. Korniienko (2020) studies the effectiveness of forensic 3D modelling of the scene using a scanner. Laser scanning is designed to create a three-dimensional model, which can be further studied to identify specific traces.

Koenig et al. (2021) explore the possibilities of using new technologies to investigate international crimes. The researchers note the importance of digital information that has been used to investigate crimes against humanity and possible war crimes using the example of the city of Timbuktu (Mali), which was destroyed because of systematic attacks. Freeman (2017) also noted the effectiveness of the use of digital technologies in cases of war crimes and crimes against humanity. The researcher reveals the peculiarities of the use of digital evidence in war crimes cases, including legislative aspects.

Shukla et al. (2020) provide a detailed description of a multivariate regression model for crime identification, analysis, and prediction. The authors make an attempt to predict crime cases and their number in one day using the example of the city of Chicago. The researchers believe that their development in the field of predicting crime will help to determine methods of preventing it, and determining the number of crimes will help to focus on specific types of crime.

The conducted literature review confirms a small number of studies on the application of innovative technologies, in particular computer simulation, in the context of military operations. At the same time, this is an important direction of research, because military operations can aggravate existing problems and cause the emergence of new ones, including the increased crime rate.

3. Methodology

3.1. Research design

According to objectives outlined in the study, the research procedure should provide for the study of the state of crime in Ukraine in order to assess whether criminal activity really tends to increase during the war; a description of the areas of application and effectiveness of forensic

computer models of offences in the context of military operations; the algorithm for developing a forensic computer model for predicting terrorist acts in the context of a military conflict; substantiating the feasibility and benefits of using the FMEA model to assess the risks of terrorist attacks in wartime.

The first stage of the study involved an analysis of the state of crime in Ukraine after the full-scale invasion of the Russian Federation (RF). The position of Ukraine in 2021, 2022 and 2023 in the ranking of crime among the countries of the world was compared for this purpose. Furthermore, it was estimated how the number of crimes by degree of severity changed in 2022 compared to 2021. The data on the number of crimes in 2021-2022 were also provided for the following categories: crimes against life and health (intentional murder, intentional grievous bodily harm, intentional moderate bodily harm, intentional minor bodily harm), violations of the laws and customs of war, proceedings on the facts of draft evasion and illegal transportation of persons across the state border (illegal transportation of persons across the state border of Ukraine, draft evasion), crimes against property (theft, robbery, fraud), offences in the field of official activity (abuse of power, declaration of false information, accepting a bribe, offering or giving a bribe).

The second stage reveals the ways in which forensic computer simulation can be applied in the context of military operations. This stage involved the creation of an algorithm for developing a forensic computer model for predicting terrorist acts in the context of a military conflict was formed.

The third stage provided for the identification and assessment of risks for the security system. For this purpose, the FMEA model was applied to evaluate terrorist attacks on the example of the frontline regions of Ukraine. The stages of the algorithm created in the previous section at which the specified model can be implemented and its purposes were identified.

3.2. Sample

The object of the study is the security system of Ukraine as a country that has been resisting a full-scale invasion of the Russian Federation for the second year in a row. The analysis of the criminogenic situation in the country confirmed the correctness of its choice as an object of research, because the number of crimes in it, particularly serious ones, increased significantly after the full-scale invasion. This leads to increasing threats to the population and national security as a whole, and requires the development of progressive approaches to combating crime.

3.3. Methods

The analysis of the state of crime in Ukraine after the full-scale invasion of the Russian Federation employed the method of statistical observation to compare the crime rate by separate categories of crimes before and after the start of military operations. The results of determining the Crime Index rating were also applied to position Ukraine among the countries of the world in terms of the crime rate. The risks and potential failures using the FMEA model were analysed to identify and assess the probability, types and consequences of terrorist attacks using the example of the frontline regions of Ukraine.

4. Results

4.1. The state of crime in Ukraine during the war

War is the most difficult trial for citizens, law enforcement agencies, the state, and the human rights protection system. In wartime, both crimes against humanity and war crimes committed by the adversary, as well as internal aggravation of the criminogenic situation, cause concern. The world ranking of the crime rate was used when determining the crime rate in Ukraine, which has been resisting the Russian invaders for the second year in a row (NUMBEO, 2023). Table 1 shows the part of the specified rating, which includes Ukraine, as well as the countries closest in terms of crime rating in 2021-2023.

Table 1. Crime Index by Country 2021-2023

Position	Country Name	Crime Index	Safety Index	Position	Country Name	Crime Index	Safety Index	Position	Country Name	Crime Index	Safety Index
2021				2022				2023			
49	Morocco	49.1	50.9	57	United States	48.2	51.8	62	Italy	47.3	52.7
50	Paraguay	49.0	51.0	58	Nicaragua	47.9	52.1	63	New Zealand	47.1	52.9
51	Iraq	48.8	51.2	59	Moldova	47.4	52.6	64	Morocco	47.1	52.9
52	Ghana	48.5	51.5	60	Greece	47.4	52.6	65	Egypt	47.0	53.0
53	Nicaragua	48.4	51.6	61	Iraq	47.0	53.0	66	United Kingdom	46.9	53.1
54	Ukraine	48.3	51.7	62	Ukraine	46.9	53.1	67	Ukraine	46.8	53.2
55	Mauritius	47.9	52.1	63	Lebanon	46.9	53.1	68	Australia	46.7	53.3
56	United States	47.7	52.3	64	Ghana	46.8	53.2	69	Barbados	46.6	53.4
57	Sweden	47.2	52.8	65	Egypt	46.6	53.4	70	Greece	46.5	53.5
58	Myanmar	47.2	52.8	66	Barbados	46.6	53.4	71	Lebanon	46.5	53.5
59	Lebanon	47.0	53.0	67	Myanmar	46.5	53.5	72	Kazakhstan	46.4	53.6

Source: created by the author based on NUMBEO (2023).

In the crime ranking given in Table 1, the higher the value of a country's position, the higher its crime rate. The overall crime rate in this ranking is calculated by dividing the total number of registered crimes of any kind by the total population and multiplying the result by 100,000 (NUMBEO, 2023). Considering that the rating includes 144 countries as of 2023, Ukraine's position can be considered quite high. The countries closest in terms of rating to Ukraine in different periods were such developed countries as the United States of America, Sweden, Italy, the United Kingdom, Australia, etc. Figure 1 illustrates the comparison of the position of Ukraine in the ranking by the crime rate before and after the full-scale invasion of the Russian Federation.

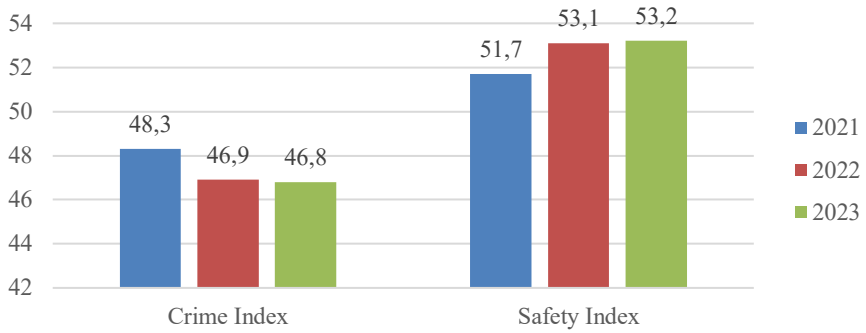

Figure 1. The position of Ukraine in the ranking by crime rate for 2021-2023

Source: created by the author based on NUMBEO (2023).

As Figure 1 and Table 1 show, Ukraine's position according to the Crime Index was higher (there was more crime) before the start of the invasion in 2022 than after it. Accordingly, the Security Index is increasing during the studied period, which could raise doubts in the context of the beginning of the war in the country. However, such a result can be explained by the fact that these indices do not take this fact into account and rely on the internal crime situation in the country only. Besides, it is most likely that the Index did not take into account the fact that a significant part of the population of Ukraine left the country after the start of the war, and therefore, there are actually more crimes per 100,000 population.

According to the Prosecutor General's Office, crime in Ukraine increased by 8.8% in 2022 (from 321,443 criminal offences in 2021 to 362,636 in 2022). At the same time, the nature of crimes has changed significantly because of the increased number of crimes against the foundations of national security, intentional killings and also war crimes, while the number of minor offences and criminal misdemeanours, offences against property has decreased (Figure 2) (Chyrenko, 2023).

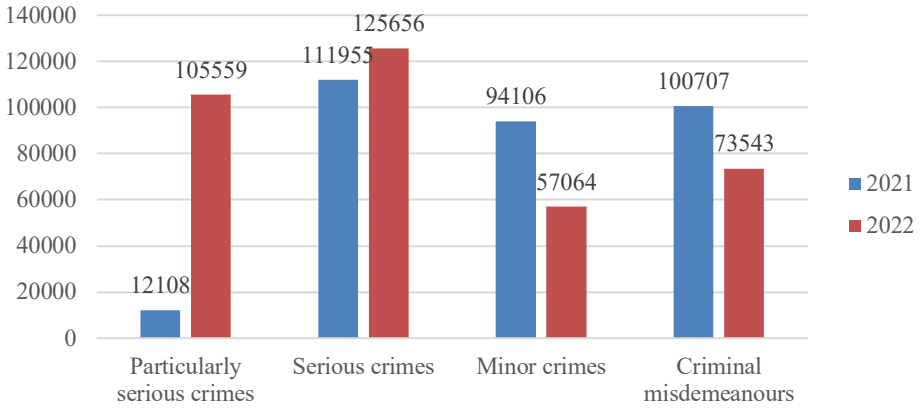

Figure 2. Data on the number of crimes by severity

Source: created by the author based on Chyrenko (2023).

As Figure 2 shows, the number of particularly serious crimes increased most significantly - almost 9 times. Table 2 indicates the number of crimes by nature.

Table 2. Number of committed crimes by nature

Nature of crime	2021	2022	Change
Crimes against life and health			
Intentional murders	3,230	22,083	+18,853
Intentional grievous bodily harm	1,601	1,502	-99
Intentional bodily harm of moderate severity	3,162	2,019	-1,143
Intentional minor injuries	19,155	13,238	-5,917
Violation of the laws and customs of war			
Violation of the laws and customs of war	172	60,387	+60,215
Proceedings on the facts of draft evasion and illegal smuggling of persons across the state border			
Illegal smuggling of persons across the state border of Ukraine	327	1225	+898
Draft evasion	-	1,108	+1,108
Crimes against property			
Theft	113,517	69,496	-44,021
Looting	4,846	2,205	-2,641
Brigandage	952	492	-460
Fraud	23,847	32,086	+8,239
Offenses in the field of official activity			
Abuse of power	3,955	2,214	-1,741
Declaring false information	-	78	+78
Accepting a bribe	1566	988	-578
Offering or giving a bribe	1,557	1,512	-45

Source: created by the author based on Chyrenko (2023).

The growing number of intentional murders and violations of the laws and customs of war deserve special attention. These statistics confirm the relevance and necessity of finding more effective ways and models for predicting, countering, and solving crimes.

4.2. The effectiveness of forensic computer models of offences in the context of military operations

Forensic computer models of offences involve the synthesis of computer programmes and analytical methods for simulation and further analysis of offences and crimes. Such models can be useful for simulating crimes and be used to fulfil different tasks in the context of military operations. In particular, it is possible to determine the following main areas of application of forensic computer models:

crime forecasting — the analysis of historical, geographical, social data about the region, as well as the analysis of economic factors, existing ethnic conflicts, living standards, conflict zones, etc. Intended for forecasting possible types of criminal events, as well as the place and time of their likely implementation in order to allocate resources to their prevention;

crime analysis – such forensic computer models are designed to analyse patterns and relationships between crimes to identify serial crimes or criminal group activity;

geo-informational simulation – modelling that takes into account geographic factors of crimes and is intended, among other things, to identify the most criminal areas;

simulation of criminal behaviour — contains an analysis of factors influencing the offenders' behaviour. A possible purpose is the creation of strategies of social influence on certain categories of citizens;

visualization — various means of visual presentation of information about crimes intended for better understanding and visibility;

investigation models — provide possible crime investigation scenarios;

process models – are intended for analysing court scenarios and predicting court decisions and other models.

The given list of possible areas of application of forensic computer models shows that such models can be used at any stage of the forensic process — from predicting crimes and preventing them to predicting court decisions. It is proposed to evaluate the effectiveness of forensic computer models using the example of building an algorithm for the development of a forensic computer model for predicting terrorist acts in the context of a military conflict.

The algorithm for developing a forensic computer model for predicting terrorist acts in the context of a military conflict involves the following stages:

Stage 1. Collecting information:

collection of historical data on terrorist acts in the studied region;

collection of geographic information and social data about the studied region, in particular, geographical location, ethnic composition, economic status, standard of living, etc.

Stage 2. Data processing:

analysis and processing of data collected at Stage 1, including detection and removal of incorrect or incomplete information;

the formation of a database by structuring the collected information about terrorist acts and the main characteristics of the studied region.

Stage 3. Identification of risk factors:

identification of factors that can influence terrorist activity in the studied region, including the distance to conflict zones, ethnic conflicts, economic indicators, etc.

Stage 4. Development of a mathematical model:

- mathematical model development based on the collected information and identified risk factors;

- model development may include methods of statistical analysis, machine learning, geoinformation systems, etc.

Stage 5. Model testing.

Stage 6. Implementation and monitoring.

Stage 7. Evaluation and analysis of the results.

Stage 8. Drawing conclusions and recommendations on improving security measures.

The generated algorithm will help to develop an effective, proven forensic computer model for predicting terrorist acts in the context of a military conflict. The effectiveness of the model depends, first of all, on the accuracy of risk identification and assessment.

4.3. Application of FMEA model for risk assessment of terrorist attacks in wartime

The success of the developed mathematical model largely depends on the correctness of identifying risks and their assessment. This paper proposes to determine the FMEA (Failure Mode and Effects Analysis) model as the basis for the development of a forensic computer model for predicting terrorist attacks in the context of military operations. This tool identifies and assesses

possible risks to the security system. The results of the application of this model can be useful for the implementation of a model for predicting terrorist attacks in the context of military operations.

The research applies the FMEA model to the assessment of terrorist attacks using the example of the frontline regions of Ukraine. The result is given in Table 3.

Table 3. FMEA model for assessing terrorist attacks using the example of the frontline regions of Ukraine

Function	Potential Failure Mode	Potential Effect(s) of Failure	S (Severity)	Potential Cause(s)	O (Occurrence)	Current Process Control	D (Detection)	RPN (Risk-Priority	CRIT (Criticality)	Recommended Actions
Protection of the city and population from terrorist threats	Invasion of armed groups or terrorists in the city	Death of civilians and military personnel	10	Terrorist acts, infiltration, subversion	9	Constant patrolling, security service	3	270	High	Strengthen border control and identification of suspicious persons
Emergency response to attacks	Lack of coordination and training	Delay in assistance and resolution of the problem	8	Insufficient training of rescue services	7	Emergency response plan	4	224	High	Conduct regular training and events with rescue services
Ensuring the safety of public transport	Terrorist attacks on public transport	Injuries and deaths of passengers	9	Explosive devices, homemade	6	Heavy police presence	4	216	High	Carry out regular inspections of transport and strengthen inspection
Protection of infrastructure facilities	Attacks on energy facilities, bridges, infrastructure	Destructions and disruptions in public life	9	Sabotage, explosions, cyber attacks	8	Guarded police facilities	4	288	Critical	Strengthen security and cyber protection of infrastructure

Source: created and calculated by the author.

Table 3 presents an assessment of functions aimed at protecting frontline regions from enemy terrorist attacks. A potential risk (Failure Mode), its possible results, and an assessment of the severity of risk realization (S) were determined for each function. Specific actions through which this risk can be realized are determined, and the occurrence (O) of such actions is estimated. The current control of the process is determined and its capabilities to detect dangerous acts (D) are assessed. Finally, RPN (Risk Priority Number), CRIT (Criticality) are calculated based on the obtained scores and recommended actions are proposed. The higher the RPN and criticality, the more urgent measures must be taken to reduce risks. The proposed measures are aimed at protecting border (front-line) cities and their citizens from terrorist attacks. In practice, after defining the measures, it is necessary to establish the time frame for their introduction, responsible persons/bodies and other criteria/resources necessary for their implementation. The implementation should be followed by evaluating the results through re-assessment S, O and D.

The obtained results can be integrated into the algorithm created above for the development of a forensic computer model for predicting terrorist acts in the context of a military conflict as follows:

at Stage 3: when identifying risk factors, the FMEA provides information for analysing potential failures and events that may lead to the realization of terrorist acts, as well as their consequences;

at Stage 4: the results of the FMEA can be applied during the development of a mathematical model to take into account potential risks in this model and determine how such risks can affect the parameters of the model;

at Stage 5: FMEA results can be integrated to analyse scenarios and events that may occur during the test period. At this stage, it is advisable to assess how correctly the model can predict and respond to probable failures and risks, and adjust it in case of inconsistencies;

at Stage 6: FMEA can be used for continuous monitoring as well as real-time risk analysis, as well as be used as a tool to identify potential failures and determine effective response measures;

at Stage 7: FMEA can evaluate the effectiveness of the analysis and the model as a whole after the implementation and monitoring, which will enable determining the ways to correct the model;

at Step 8: the results of the FMEA analysis can provide ample scope for developing recommendations for regulators, law enforcement, the military, and the public.

So, FMEA can be integrated at almost every step of the algorithm. This will increase the effectiveness of the developed model and enable monitoring and evaluation of results. An

important condition for success in the development of the model is the coordination of the work of law enforcement agencies and computer technology specialists.

5. Discussion

According to Sokurenko (2022), the promising directions of the development of criminology include the creation and adaptation of different information technologies to the fulfilment of criminology tasks, non-contact emotion recognition technologies, the development of the skills of detecting virtual traces in investigators and the ability to work with various electronic media and other modern technologies, the introduction of new technologies in practice etc. The analysis carried out in the author's article indicates that the implementation of the mentioned directions is impossible without effective cooperation between law enforcement officers and computer specialists, which should be singled out as a separate direction.

Podobnyi and Slatvinska (2021) list the main tasks of informatization of law enforcement activities, including: filling databases and providing access to them for law enforcement officers, applying analytical methods for processing information and resources of non-departmental information systems, monitoring trends in the development of crime, adapting tactics and methods of crime investigation to modern conditions of informatization, integration into the specialized software. Unlike the author's research, the researchers focus on cybercrime. However, the author's work suggests that the latest information technologies can be equally useful for the prediction and prevention of non-cybercrime offences.

Casey (2019) recommends bridging the gap between forensics and digital forensics and harmonizing these fields through the application and collaboration of two roles: an investigative advisor with relevant work experience and a forensic advisor with the necessary training. The activities of these specialists will help ensure more effective communication and cooperation between digital forensics specialists, police, analysts and lawyers, which will ultimately ensure the development of the criminal justice system as a whole. Jarrett and Choo (2021) believe that digital forensics will receive significant benefits from: receiving budget funds to expand the capabilities of digital forensics, taking into account existing threats and vulnerabilities; encouraging cooperation between developers of new technologies and digital forensics specialists; investment in improving cyber security; implementation of automation, security analysis and advanced analytics to minimize threat identification costs; raising the awareness of citizens, organizations, law enforcement agencies and other participants. Dasaklis et al. (2021) propose to apply blockchain technology in

digital forensics, which will contribute to the solution of a number of existing problems. According to the researchers, such problems include interaction, multi-jurisdictional powers, a large amount of evidence and interested parties. These studies confirm the author's hypothesis about the possibility and appropriateness of using information technologies in the investigation of crimes of any nature, and the importance of cooperation between law enforcement agencies and computer technology specialists.

Jafari and Satti (2015) compare a number of digital forensics process models based on the presence or absence of certain stages, including: data collection, study, analysis, reporting, preparation, strategy/approach, data preservation, presentation, return/evidence, decision, review, reconstruction , documentation, authorization, survey, tracking, communication, research, testing. According to researchers, the SRDFIM model contains the optimal set of stages, because it is the most complete and the only one that has such an important stage as "communication" among the models studied by the researchers. In contrast to this study, in the author's work, communication was not singled out as a separate stage during the development of the model algorithm. In the author's opinion, communication is not a separate stage, but should accompany the entire model development process as a connecting link between all stages.

Korniienko (2020) notes the effectiveness of forensic 3D modelling of the scene. Such modelling provides the following advantages: reduction of time for recording data, measuring and photographing, the ability not to lose individual details and to conduct a detailed analysis. Their work deals with modelling post factum, when the crime has already occurred. The model proposed in the author's research is aimed at predicting crimes.

Koenig et al. (2021) provides the example of an investigation into crimes against humanity and possible war crimes in Timbuktu. This investigation used digital information, such as photos and videos of the buildings before and after their destruction, satellite imagery that allowed these photos and videos to be placed in geographic space. In addition, a digital platform was used that enabled a better understanding of how pieces of visual evidence fit into a geographic space. Freeman (2017) observes that witness statements are no longer the only evidence in the investigation of crimes against humanity and war crimes thanks to the possibility of using digital evidence. In the cases discussed in the article, evidence was obtained through the criminals' use of mobile phones, their publication of video materials containing propaganda, the use of e-mail for communication, as well as through bank transfers. These works also reveal how computer technology can be useful during the investigation, after crimes have been committed. The model proposed by the author of this article aims to predict and prevent terrorist acts.

Shukla et al. (2020) developed a multivariate regression model for crime identification, analysis, and prediction. The researchers processed online crime information in the study area, identified geographic crime locations and police stations, visualized latent associations and observations, then generated a series of predictions and developed the model. The crime count was designed to identify the most frequent offences in order to focus on them and increase inspections of areas with the highest crime rates. The researchers focused on everyday factors of crime, not taking into account the causes of crimes (political reasons, criminal origin of criminals, etc.). In contrast to this study, the causes of crime play an important role in determining risk factors in the author's research.

6. Conclusions

The aggravation of global conflicts and the increasing terrorist threats is a characteristic feature of the current geopolitical situation. Incentives of various origins arise in these conditions, causing an increase in the crime rate and criminal activity. Such processes lead to increased danger for citizens and the state and require appropriate actions in response to increased risks. One of the actual methods of countering the growth of crime is the method of forensic computer simulation.

The conducted research confirmed that the war in the country is a trigger for the increase in the level of crime, in particular, the number of particularly serious crimes. As the example of Ukraine shows, the number of particularly serious crimes after the full-scale invasion of the Russian Federation increased almost 9 times, from 12,108 in 2021 to 105,559 in 2022. In response to such processes, appropriate measures, including innovative ones, must be introduced into the activities of law enforcement agencies. As it was established in the study, the method of forensic computer modelling of offences can be applied for forecasting and analysis of crime, geo-informational simulation, and other measures to combat and overcome crime. It was also determined that the success of the application of this method largely depends on the correct identification and assessment of potential risks. For this purpose, the study proposes to include the FMEA model in the algorithm for developing a forensic computer model for predicting terrorist acts in the context of a military conflict. It was found that this model is useful and can be implemented in fact at any stage of the algorithm for predicting and assessing risks and probable failures, as well as developing appropriate strategies and propositions.

The results of the study can be useful for law enforcement agencies to optimize their activities by using the FMEA model for risk prediction. Further research may be related to the possibilities of using forensic computer simulations to counter war crimes committed by the adversary.

References

AL-DHAQM, A., ABD RAZAK, S., OTHMAN, S. H., ALI, A., GHALEB, F. A., ROSMAN, A. S., MARNI, N. Database forensic investigation process models: A review. **IEEE Access,** v. 8, p. 48477-48490, 2020. https://doi.org/10.1109/ACCESS.2020.2976885

BABUTA, A., OSWALD, M. **Data analytics and algorithms in policing in England and Wales: Towards a new policy framework.** 2020. Available at: http://nrl.northumbria.ac.uk/id/eprint/42903 Accessed on: 05 Nov. 2023.

BEN HASSEN, T., EL BILALI, H. Impacts of the Russia-Ukraine war on global food security: towards more sustainable and resilient food systems? **Foods**, v. 11, n. 15, p. 2301, 2022. https://doi.org/10.3390/foods11152301

BOUBAKER, S., GOODELL, J. W., PANDEY, D. K., KUMARI, V. Heterogeneous impacts of wars on global equity markets: Evidence from the invasion of Ukraine. **Finance Research Letters**, v. 48, p. 102934, 2022. https://doi.org/10.1016/j.frl.2022.102934

CASEY, E. The chequered past and risky future of digital forensics. **Australian Journal of Forensic Sciences**, v. 51, n. 6, p. 649-664, 2019. https://doi.org/10.1080/00450618.2018.1554090

CHYRENKO, M. **Another side of the coin: how the war affected the crime rate.** 2023. Available at: https://www.dsnews.ua/ukr/politics/shche-odin-bik-medali-yak-viyna-vplinula-na-riven-zlochinnosti-27022023-475107 Accessed on: 05 Nov. 2023.

DALY, S. Z., PALER, L., SAMII, C. Wartime ties and the social logic of crime. **Journal of Peace Research**, v. 57, n. 4, p. 536-550, 2020. https://doi.org/10.1177/0022343319897098

DASAKLIS, T. K., CASINO, F., PATSAKIS, C. SoK: Blockchain solutions for forensics. In **Technology Development for Security Practitioners**. Cham: Springer, 2021, p. 21-40. https://doi.org/10.1007/978-3-030-69460-9_2

FREEMAN, L. Digital evidence and war crimes prosecutions: the impact of digital technologies on international criminal investigations and trials. **Fordham Int'l LJ**, v. 41, p. 283, 2017. Available at: https://ir.lawnet.fordham.edu/ilj/vol41/iss2/1 Accessed on: 05 Nov. 2023.

GOSTIN, L. O., RUBENSTEIN, L. S. Attacks on health care in the war in Ukraine: International law and the need for accountability. **JAMA,** v. 327, n. 16, p. 1541-1542, 2022. https://doi.org/10.1001/jama.2022.6045

HO, H., KO, R., MAZEROLLE, L. Situational Crime Prevention (SCP) techniques to prevent and control cybercrimes: A focused systematic review. **Computers & Security**, v. 115, p. 102611, 2022. https://doi.org/10.1016/j.cose.2022.102611

HOANG, N. D., HUYNH, T. C., TRAN, V. D. Computer vision-based patched and unpatched pothole classification using machine learning approach optimized by forensic-based investigation metaheuristic. **Complexity**, v. 2021, p. 1-17, 2021. https://doi.org/10.1155/2021/3511375

JAFARI, F., SATTI, R. S. Comparative analysis of digital forensic models. **Journal of Advances in Computer Networks**, v. 3, n. 1, p. 82-86, 2015. https://doi.org/10.7763/JACN.2015.V3.146

JARRETT, A., CHOO, K. K. R. The impact of automation and artificial intelligence on digital forensics. **Wiley Interdisciplinary Reviews: Forensic Science**, v. 3, n. 6, p. e1418, 2021. https://doi.org/10.1002/wfs2.1418

JIN, G., WANG, Q., ZHU, C., FENG, Y., HUANG, J., ZHOU, J. Addressing crime situation forecasting task with temporal graph convolutional neural network approach. In: **2020 12th**

International Conference on Measuring Technology and Mechatronics Automation. IEEE: 2020, p. 474-478. https://doi.org/10.1109/ICMTMA50254.2020.00108

KOENIG, A., IRVING, E., MCDERMOTT, Y., MURRAY, D. New technologies and the investigation of international crimes: An introduction. **Journal of International Criminal Justice**, v. 19, n. 1, p. 1-7, 2021. https://doi.org/10.1093/jicj/mqab040

KOLLA, V. R. K. A Comparative Analysis of OS Forensics Tools. **International Journal of Research in IT and Management**, v. 12, n. 4, 2022. Available at: https://ssrn.com/abstract=4413730 Accessed on: 05 Nov. 2023.

KORNIIENKO, V. V. Forensic 3D modeling of the scene. In: **Theoretical issues of jurisprudence and problems of law enforcement: challenges of the 21st century. Theses of the reports of the participants of the 3rd All-Ukrainian Scientific and Practical Conference.** Public Policy and Social Sciences Research Institute, 2020, p. 165-167. Available at: https://dspace.univd.edu.ua/server/api/core/bitstreams/e2172522-77cc-48a2-bcb2-aa47fec76578/content#page=165 Accessed on: 05 Nov. 2023.

KUMAR, S., PATHAK, S. K., SINGH, J. A Comprehensive Study of XSS Attack and the Digital Forensic Models to Gather the Evidence. **ECS Transactions**, v. 107, n. 1, p. 7153, 2022. https://doi.org/10.1149/10701.7153ecst

MBAH, R. E., WASUM, D. F. Russian-Ukraine 2022 War: A review of the economic impact of Russian-Ukraine crisis on the USA, UK, Canada, and Europe. **Advances in Social Sciences Research Journal**, v. 9, n. 3, p. 144-153, 2022. https://doi.org/10.14738/assrj.93.12005.

MILIVOJEVIC, S., RADULSKI, E. M. The 'future Internet' and crime: towards a criminology of the Internet of Things. **Current Issues in Criminal Justice**, v. 32, n. 2, p. 193-207, 2020. https://doi.org/10.1080/10345329.2020.1733452

NUMBEO. **Crime Index by Country 2023.** 2023. Available at: https://www.numbeo.com/crime/rankings_by_country.jsp Accessed on: 05 Nov. 2023.

OZKAN, T. Criminology in the age of data explosion: New directions. **The Social Science Journal**, v. 56, n. 2, p. 208-219, 2019. https://doi.org/10.1016/j.soscij.2018.10.010

PODOBNYI, O. O., SLATVINSKA, V. M. Main tasks of informatization of law enforcement activities. **Juridical Scientific and Electronic Journal**, v. 9, p. 180-182, 2021. https://doi.org/10.32782/2524-0374/2021-9/43

PRATHAP, B. R. Geospatial crime analysis and forecasting with machine learning techniques. In: **Artificial intelligence and machine learning for EDGE computing**. Academic Press, 2022, p. 87-102. https://doi.org/10.1016/B978-0-12-824054-0.00008-3

RAWTANI, D., GUPTA, G., KHATRI, N., RAO, P. K., HUSSAIN, C. M. Environmental damages due to war in Ukraine: A perspective. **Science of the Total Environment**, v. 850, p. 157932, 2022. https://doi.org/10.1016/j.scitotenv.2022.157932

REN, L., ZHAO, J. S., HE, N. P. Broken windows theory and citizen engagement in crime prevention. **Justice quarterly**, v. 36, n. 1, p. 1-30, 2019. https://doi.org/10.1080/07418825.2017.1374434

SHUKLA, S., JAIN, P. K., BABU, C. R., PAMULA, R. A multivariate regression model for identifying, analyzing and predicting crimes. **Wireless Personal Communications,** v. 113, p. 2447-2461, 2020. https://doi.org/10.1007/s11277-020-07335-w

SOKURENKO, V. V. Peculiarities of the use of information technologies in forensics. In: **Application of information technologies in law enforcement activities: materials of the Round Table.** Kharkiv: KhNUVS, 2022, p. 8–12. Available at: http://dspace.univd.edu.ua/xmlui/handle/123456789/15146 Accessed on: 05 Nov. 2023.

XU, Z., CHENG, C., SUGUMARAN, V. Big data analytics of crime prevention and control based on image processing upon cloud computing. **Journal of Surveillance, Security and Safety**, v. 1, p. 16-33, 2020. https://doi.org/10.20517/jsss.2020.04