

Assistant lecturer Ágota NÉMETH¹
University of Public Service, Faculty of Law, Hungary
Associate professor Vince VARI, PhD²
University of Public Service, Faculty of Law,
Department of Criminal Procedure, Hungary

DOI: 10.5937/bezbednost2403097N

UDK: 343.98:004.62

004.8:343.98

Pregledni naučni rad

Primljen: 19. 4. 2024. godine

Revizija: 20. 10. 2024. godine

Datum prihvatanja: 21. 10. 2024. godine

The Dilemmas of Criminal Intelligence Analysis

Abstract: *The authors in the paper examine the biases and errors that can arise in criminal analysis using human power and artificial intelligence and their impact on the final product of the analysis process. Also, the authors research the international literature on forensic analysis to determine how artificial intelligence can be used in addition to extensive data analysis to perform analytical tasks in evidence gathering in the form of mass data. There may be forensic and human analytics analysis errors, mainly related to the subject. These errors are also valid for AI analysis, where human power is also present, from the algorithms' design to the analysis's end. The subject's topicality is unquestionable, as we are faced with an ever-increasing amount of information that is almost impossible to process using human power.*

Keywords: *criminal analysis, criminal analysts, artificial intelligence.*

Introduction

Crime and criminals can be investigated with an activity known as crime analysis. Crime analysis is defined "as the systematic study of crime and disorder problems as well as other police-related issues - including

¹ nemeth.agota@uni-nke.hu

² variv@uni-nke.hu

sociodemographic, spatial, and temporal factors - to assist the police in criminal apprehension, crime and disorder reduction, crime prevention, and evaluation" (Boba, 2005: 5).

The following types of crime analysis can be distinguished: intelligence analysis, criminal investigation analysis, tactical crime analysis, strategic crime analysis, and administrative crime analysis (Otašević, 2015: 2017). Crime analysts examine the relationship between the criminal and the individual crime, analysing the profile of the offender, the way the crime was committed, and the location of the crime (Boba, 2005: 14). Operational/tactical crime analysts look at recent criminal events, while strategic crime analysts focus on longer-term crime problems. Administrative crime analysts review previous analyses, find interesting facts, and then compile them in various formats to inform the public about specific crimes (Boba, 2005: 16).

The last decades of the 20th century saw the emergence of an approach in the activities of law enforcement agencies to not only react to violations (Čvorović et al., 2021) that have occurred, but to replace the reactive approach with a preventive, deterrent approach and to try to detect criminal risks earlier.

This period has seen and continues to see the explosion of computer and telecommunications technology. The flow of information and communication has become even faster and a wide range of data storage devices have become more widely available. With the emergence of the pandemic, the online space has become even more pronounced, with cyberspace increasingly becoming the place where crime is committed. This process continues today. In the world of the Internet, we need to talk about the darknet, which is a network of networks that are not easily accessible to anyone with open access. Part of the darknet is the darkweb, which is a platform for illegal and infringing activities. The primary goal here is to extract data that can be used to further search the open web.

It also generates an increasing amount of information, covering a large, extremely varied, complex, and rapidly changing amount of data. These characteristics already suggest that these data volumes can no longer be managed by traditional tools such as database managers, and that systematic data analysis cannot be performed. To process

them, artificial intelligence technologies are needed. Methods, tools and applications designed specifically for Big Data analysis that can be used to collect, process, and derive analyses from different, large, high-volume, high-velocity data sets play an important role in this, according to the Microsoft website. These data sets can come from a variety of sources, such as the web, mobile devices, email, social media and smart grid devices. They often contain high velocity data, which can be in a wide variety of formats, ranging from structured data (such as database tables or Excel worksheets) to semi-structured data (XML files, web pages) and unstructured data (images, audio files).

Despite the changes, the criminals of the modern age are still up to date in the world of technology and the Internet, and they use the results of their work very quickly and skilfully, which the authorities must constantly adapt to, as this is the only way to fight them effectively. New technologies and methods must also be used in the field of criminal analysis to make police work more effective.

The older approach to crime statistics, which was used to improve understanding, employed simple mathematical techniques in its methodology. However, this method is mainly applicable to data that is both small in size and complex. In contrast, predictive policing requires sophisticated analytical methods because it performs calculations on large and complex data sets. Both the data collection and processing, as well as the tasks defined on the basis of the data need to be up-to-date, which is not always an easy task when dealing with huge amounts of data.

Criminal intelligence analysis

Criminal intelligence analysts are tasked with producing strategic or operational intelligence products that are used to meet various police objectives. The purpose of strategic intelligence is to inform appropriate changes and developments in police policies, programs, and legislation, nationally or internationally. The findings generated from the ongoing analysis of information obtained in the intelligence cycle enable law enforcement agencies to respond promptly to an identified crime situation at the local level (UNODC, 2011: 9).

Operational analysis can be divided into two parts: mass crime analysis and serious crime analysis. The mass crime analysis covers crimes that occur in large numbers and have a significant impact on the community, making it difficult for local police to act. Examples of such crimes include street robbery, burglary, and vehicle crime. The analysis of serious crime focuses on crimes that involve violence, high financial gain, or are committed by large numbers of people for a common purpose. Examples of such serious crimes include murder and drug trafficking (Selvaraj et al., 2016).

The concept of information used in criminal analysis is not the same as the general definition of information, where information always has some criminal content, relevance, and is adapted to the needs of the user. The information obtained by criminal intelligence services from different sources, using different methods and tools, must be examined, evaluated, and classified according to its value, since information has professional and material value.

A distinction must be made between raw and analysed information from several points of view. Raw information is fresh, current, and requires further verification. The source, content, timeliness, linkage to existing information, and usability of the information should be checked. Analysed information must be verified, classified, checked against other sources, supplemented, clarified, and usable.

One of the fundamental differences between raw and analysed information is that analysed information goes through a verification mechanism and is then supplemented with existing knowledge to give it a new value, a higher quality, especially in terms of usability (ACPO/Centrex, 2007).

Methods and techniques used by criminal intelligence analysts

A forensic analysis method is a set of analytical techniques and the way in which they are used, in an appropriate sequence, to achieve the result to be obtained, in accordance with the principles.

Crime pattern analysis is the study of the number, characteristics and changes in the number of crimes (all or certain categories of crimes) in a

given geographical area over a given period of time. In addition to a general description of the phenomenon, it examines the cause of the events, the relationship between events and characteristics, and the impact of police activity on the phenomenon (Hajela et al., 2020: 1465). Similar but not identical to, and not part of, crime pattern analysis is trend analysis, which analyses the direction and causes of quantitative and qualitative change in all crimes or in certain types of crime.

By processing data on offenders and victims of crime, general profile analysis provides a picture of the typical offender, the typical perpetrator of each category of crime, the typical victim, who becomes a victim of crime and why.

The risk analysis identifies the actual events with potential negative effects and their causes, then ranks them according to the likelihood of occurrence and the extent of the damage caused, and formulates countermeasures that can be taken to achieve risk-based protection.

The threat analysis identifies current and anticipated security risks, including social, economic, political, and other factors that influence crime, and then identifies various priorities.

Case analysis is a reconstruction of the process of committing a crime, examining the activities of the people involved. Comparative case analysis is an assessment of the elements of crimes committed by similar methods, in similar places, at similar times, and on similar subjects, to determine whether they can be considered as a series.

Offender-group analysis can reveal the activities of criminal groups, the division of tasks between their members, and their further relationships.

The analysis of communication links reveals the frequency, duration, and patterns of communication by telephone and the Internet.

The social network is constructed by exploring the interrelationships between persons, relationships, and roles, where various events, information, emotions, and material things are exchanged. The analysis may also include exploring financial and economic relationships, in addition to personal and communication relationships.

The primary purpose of financial transaction analysis is to reconstruct financial transactions on a timeline, but it also helps to map relationships (Németh, 2022).

Above, I have described the most commonly used analysis tasks, and a brief description of each of them shows that a large amount of data can be the basis for the analysis of an analysis task.

The forms and methods of forensic analysis are supported by the applied forensic analysis techniques, which are forms of representation of relationships and connections between individuals, events, and other information objects. An internationally standardized system of symbols has been developed for this purpose. Starting from manual representation, various computer-based representations and techniques have been developed, incorporating the principles and notation techniques developed during manual analysis.

Statistically based visualization techniques include various statistical tables, charts, dot and dot plots, and organization charts. On the other hand, operational representation techniques encompass a narrower range of individual cases, such as forensic tables, relationship matrices, relationship diagrams, flow charts, event diagrams, flow charts, event maps, time graphs, images, and videos.

While these tools can be used with traditional media like pen and paper, there are also commercial software applications available. One such tool is IBM i2 Analyst's Notebook, which is widely used in analysis departments worldwide. It enables network and complex analyses based on a pre-existing information database, as well as individual analyses. The tool allows for the management of data from different sources in a standardized manner and the linking of data tables. In addition to visualizing individual crimes, it can also be utilized to depict various relationships and display events in chronological order, aiding in the detection of organized crime groups.

Cope argued that although there are various tools and analytical techniques available for analysis, criminal analysis is a highly subjective process. The reason for this is that criminal analysts use the same analytical techniques to produce the analytical product of crime analysis, which form the basis for representing the relationships between the information available during the analytical process and for drawing conclusions (Cope, 2004: 192).

The purpose of visual analytics is to assist the analytical reasoning process by facilitating the review and understanding of the analysis. In analytical reasoning, analysts use the available data information to justify hypotheses, i.e. to draw conclusions from a combination of evidence and assumptions (Thomas, Cook, 2005).

There is an ongoing dialogue between analysts and information. This dialogue is an iterative process of making judgments about issues and is referred to as analytic discourse. The intelligence cycle is cyclical and subjective, as there is a personal interaction between the analyst and the information. Supporting analytic discourse requires an understanding of the thought process (Cope, 2004: 196).

The dilemmas of human power analysis

The "investigative mindset" is based on the ABC rule, which means assuming nothing, believing nothing, and checking everything. This rule serves as an itinerary for investigators and analysts to pay particular attention to the assumptions they make based on their existing experience and knowledge. A hypothesis is an assumption based on the primary available data and information that serves as the starting point for analysis (Cook et al., 2013).

The process of using knowledge is called heuristics. The heuristic theory is designed to allow the association of given circumstances with past examples to help the analyst make effective and appropriate decisions (Cook et al., 2013).

The heuristic has a specific role in cases where there is limited or no clear information available, and the analyst relies on previous knowledge and experience to fill in these gaps and continue the analysis.

If heuristics are present, cognitive biases will appear. Heuer describes cognitive biases as mental errors caused by our simplified information processing strategy. Cognitive biases do not arise from the emotional or intellectual content of a given judgment, but from the possible mental process of processing information. Heuer outlines that there are other biases, such as cultural, organizational bias, and bias based on self-interest.

An initial impression is formed by the analyst when examining the available data and information, identifying and representing the relationships between them, and this impression is likely to persist even if new information or evidence contradicts their initial impression. This confirmation bias is particularly common when only one hypothesis is proposed (Heuer, Pehrson, 2015).

There is a risk that crime analysts, in the process of analysis, do not make use of information requests to intelligence officers, and also that they find it difficult to judge how this is currently being used to reconstruct the historical facts in the absence of information (Heuer, Pherson, 2015),

Heuer further points out that forensic analysts tend to accept all information as valid, even if only some of it is factual or ambiguous in nature. Heuer also notes that analysts often fail to verify new information and fit it into the set of relationships of existing information. This also manifests itself in judging situations from their own perspective, ignoring the intentions of the perpetrators (Heuer, Pherson, 2015).

In addition to human factors, one other case of bias in criminal analysis that is nowadays claiming space almost everywhere is that of bias. This is artificial intelligence.

Artificial intelligence

The use of Artificial intelligence (AI) systems poses new challenges for law enforcement users. On the one hand, AI systems offer the opportunity for optimization and faster workflows, especially with increasing amounts of data. On the other hand, if left unchecked, these systems can have a number of negative effects on law enforcement.

The integration of AI into police systems can be implemented in a number of areas that can help law enforcement. Police officers can request information from the AI system about crime or suspicious activity. AI can help to quickly search and analyze crime data, and can provide the opportunity to analyze and evaluate crime data, for example, based on crime statistics or offender patterns. It can help law enforcement authorities to understand and prevent crime. The AI system can help in the analysis of textual information during investigations, for example, to interpret

suspicious messages. It can provide up-to-date information on some ongoing open investigations, local crime trends, and emerging threats.

The use of artificial intelligence in law enforcement

Law enforcement agencies are no strangers to the use of AI systems. Starting in the 2020s, a number of IT companies will be developing software that can support various law enforcement activities with AI support. These may include advanced applications for data analysis, image and video analysis systems, and programs for predictive analytics to support predictive policing. While these programs do not fully exploit the full potential of AI, they seek to apply only the most common and up-to-date models of use to law enforcement.

A review of the international literature shows the following areas where AI is most commonly used in law enforcement to support law enforcement and crime prevention.

Data collection and analysis

Open source information collection and text mining methods help to automatically analyze and process information. The tools allow related data to be organized in a structured form that can be easily and quickly searched, data can be linked, and a faster response to specific phenomena and trends is possible.

Mapping of offender contact networks, further development of the graph database

Analysis with AI support will collect specific data, including telephone conversations, emails, social media posts, GPS tracking data and bank transaction data. During the analysis and processing of the data, AI algorithms detect and map networks of contacts that show the links between individual criminals and their level of organisation (URL1).

Automated License Plate Readers

Automated number plate readers enable the automation of number plate runs to identify whether a vehicle is associated with various alarms, wanted persons, stolen vehicles or other signals. This also allows the police to take action in real time based on the license plate recognition, if the system predicts the direction of the vehicle being searched (Roberts, Casanova, 2012).

Facial Recognition

The surveillance cameras are also important in assisting police work, as they can identify people who are moving around in a given area at a given time. The advantage of facial recognition is that the person to be identified does not need to be aware of its use. By analysing the cameras and their networks, the presence of people can be analysed, which can be used to obtain an account of an individual's activity, movements, daily routine and behaviour (Dharaiya, 2020).

Predictive Analytics

Predictive analytics "uses techniques ranging from machine learning, statistics, data mining, modelling and AI to analyze current data and make predictions about the future" (Kavya, Aruguman, 2016). In the field of law enforcement, predictive analytics can also be used to predict where and when future incidents are most likely to occur (Malik et al, 2014, 1684). In addition to predicting when crime will occur, AI can also help identify high-risk individuals from the behavioral patterns of individuals, and can be used to group individuals by analyzing behavioral data from various sources.

In addition to the above, there are other areas of research in AI that can also support the work of the police. Examples include real-time image analysis using drones, or the collection, structuring, and analysis of data from different sources by AI.

The key to the involvement of AI in crime analysis is to establish the appropriate legal framework and to take into account the negative impact of the biases described above on the analysis.

Dilemmas of using artificial intelligence

The ever-increasing volume of data generated requires law enforcement agencies to adapt to new technical challenges. Data analysis, graphing, facial recognition, predictive risk assessment, and predictive policing AI systems perform different tasks and provide different outputs for law enforcement. However, all of these applications have the same problem, the most significant of which is inaccuracy. This can lead to innocent people being suspected of crimes they did not commit. Facial recognition systems using AI can create various biometric databases in the course of their operation, which can include both innocent and criminal individuals. When facial recognition is used in live video feeds, the requirements of anonymity or privacy standards almost erode the capabilities of facial recognition systems.

Most AI systems lack transparency. A "black box" environment does not allow outside parties to understand how the system works. As a result, vendors often make proprietary claims or are unable to explain how the AI system arrived at easily understood results. The lack of transparency makes the functioning of the AI system less understandable. The situation is further exacerbated when law enforcement agencies use these "black box" systems, as they may have difficulty explaining the reasoning behind the conclusions (Rouse, 2019).

The European Commission's AI HLEG (AI HLEG) has established a legal framework that defines the ethical aspects, principles, basic requirements, and evaluation methods for the implementation of sound AI in the European Union. The AI HLEG has emphasized that the application of AI systems must be guided by ethical principles of respect for human autonomy, without which AI can pose significant risks to individuals and groups that are difficult to foresee (URL2).

It is in this spirit that the European Parliament adopted its Regulation on AI on 21 May 2024. The primary objective of this norm is to protect

fundamental rights and the rule of law against high-risk AI. The Regulation sets out obligations for MI based on the potential risks and their extent. Accordingly, where there is an unacceptably high risk, it prohibits the use of MI in certain areas that also involve the analysis of crime, such as certain types of predictive policing. Prohibited areas of application include face scanning by police in public using remote biometric identification systems with the aid of AI, except for serious crimes such as terrorism or kidnapping (URL2).

Conclusion

Criminal intelligence and investigations require increasingly specialised knowledge. More and more specialised information needs to be systematised and processed, which increasingly requires the application of analytical methods and techniques, the professional and technical development and further specialisation of the field of crime analysis. In particular, law enforcement, and criminal analysis in particular, is a constantly evolving branch of police work which never stops and never catches up with crime.

Even in the analysis of crime, i.e. by human power, there can be errors and distortions, which are primarily related to the subject. Does this bias apply in the case of AI analysis, where human power is also present in the design of algorithms for the program, in the selection of learning data, decision criteria and in the evaluation of the result?

Law enforcement around the world in the 21st century faces the same problem: in the face of exponential growth in data, there is a limited human resource available (Hollywood, 2018). The application of AI systems can make up for this shortage of manpower to a significant extent (see facial recognition, machine learning). It can also speed up workflows and increase efficiency in many police departments. But it can also have negative effects, e.g. inaccuracy, bias, and errors that are not primarily validated (Osoba, Welser, 2017).

Based on the above, it can be stated almost entirely that the automated application of AI in the field of police work, law enforcement, and crime analysis is not possible and can only be used under the control of human

resources. Guarantees must be put in place that the final decision in the field covered by the AI is always taken by the human force, i.e. the human being.

In the future, police departments, particularly analytical units, will integrate various technologies in different areas of police work. Advances in technology require that police departments' crime analysts become more skilled and professional. Crime analysis, crime analysts are an increasingly indispensable resource in today's law enforcement agencies. It is predicted that the role of crime analysts will continue to grow as technology advances (Taylor-Francis, 2020).

References

1. ACPO/CENTREX (2007). *Practice Advice - Introduction to Intelligence-Led Policing*, <http://www.fairplay31.epizy.com/pdf/1291430265.pdf?i=1>. available on 11. 11. 2023
2. Boba, R. (2005). *Crime analysis defined. Crime analysis and crime mapping*, 5:18, https://www.sagepub.com/sites/default/files/upm-binaries/6243_Chapter_2__Boba_Final_PDF_2.pdf available on 11. 11. 2023.
3. Cook, T., Hibbitt, S., Hill, M., (2013). *Blackstone's Crime Investigator's Handbook*. Oxford University Press.
4. Cope, N. (2004). 'Intelligence Led Policing or Policing Led Intelligence?' Integrating Volume Crime Analysis into Policing. *British journal of criminology*, 44(2): 188-203.
5. Čvorović, D., Otašević, B., Vranešević, M., (2021). Multisektorska saradnja u slučajevima nasilja u porodici iz ugla centra za socijalni rad. *Sociološki pregled*, 55(3): 1138-1163
6. Dharaiya, D. (2020). "History of Facial Recognition Technology and Its Bright Future." readwrite, March 12. 2020, <https://readwrite.com/2020/03/12/history-of-facial-recognition-technology-and-its-bright-future/>. available on 11. 11. 2023
7. Hajela, G., Chawla, M., Rasool, A., (2020). A clustering based hotspot identification approach for crime prediction. *Procedia Computer Science*, 167: 1462-1470.

8. Heuer, R. J., Pherson, R. H., (2015). *Structured techniques for intelligence analysis*. SAGE Publications. USA.
9. Hollywood, J., Woods, D., Laland, A., Jackson, B., Silberglitt, R. (2018). *Addressing Emerging Trends to Support the Future of Criminal Justice: Findings of the Criminal Justice Technology Forecasting Group*, Santa Monica, CA: RAND, https://www.rand.org/pubs/research_reports/RR1987.html available on 18. 12. 2023.
10. Kavya, V., Arumugam, S. (2016). A Review on Predictive Analytics in Data Mining. *International Journal of Chaos, Control, Modelling and Simulation* 5(1): 1–8. <https://airccse.org/journal/ijccms/papers/5316ijccms01.pdf> available on 19. 11. 2023.
11. Malik, A., Maciejewski, R., Towers, S., McCullough, S., Ebert, D. (2014). “Proactive Spatiotemporal Resource Allocation and Predictive Visual Analytics for Community Policing and Law Enforcement”, *IEEE Transactions on Visualization and Computer Graphics* 20, 12: 10. https://vis.cs.ucdavis.edu/vis2014papers/TVCG/papers/1863_20_tvcg12-malik-2346926.pdf available on 18.11.2023.
12. Németh, Á. (2022). *A bűnügyi elemző-értékelő munka. (Knowledge of the criminal services)*, In conference proceedings “Bűnügyi szolgálati ismeretek Különös rész”, Ludovika Egyetemi Kiadó, Budapest, p. 215–234.
13. Otašević, B. (2015). *Nasilje na sportskim priredbama*. Službeni glasnik, Beograd.
14. Osoba, O., Welser, W. (2017). *An Intelligence in Our Image: The Risks of Bias and Errors in Artificial Intelligence*. Santa Monica, CA: RAND Corporation, https://www.rand.org/pubs/research_reports/RR1744.html. Available on 18. 11. 2023. <https://www.ojp.gov/pdffiles1/nij/grants/239605.pdf> available on 19. 12. 2023.
15. Roberts, D. J., Casanova, M. (2012). *Automated License Plate Recognition (ALPR) Use by Law Enforcement: Policy and Operational Guide, Summary*. 239605. Alexandria, VA: International Association of Chiefs of Police, <https://www.ojp.gov/pdffiles1/nij/grants/239605.pdf> available on 19. 12. 2023.
16. Rouse, M. (2019). “What Is Black Box AI?” *What Is*, <https://www.techopedia.com/definition/34940/black-box-ai> available on 18. 12. 2023.

17. Selvaraj, N., Attfield, S., Passmore, P., Wong, B.W., (2016). *How Analysts Think: Think-steps as a Tool for Structuring Sensemaking in Criminal Intelligence Analysis*, In conference proceedings “Intelligence and Security Informatics Conference (EISIC)”, IEEE, p. 68-75 <https://repository.mdx.ac.uk/download/453352eaefef6f454bc4302b3bb901910d3a729a4d95ea9e8ee259bf634d1cdc/186341/2016%20Selvaraj%20Attfield%20Passmore%20%26%20Wong...%20How%20Analysts%20Think-ThinkSteps%20as%20a%20Tool%20for%20Sensemaking%20in%20Criminal%20Intelligence%20Analysis.pdf> available on 18.11.2023
18. Thomas J.J. and Cook K.A. (2005). *Illuminating the Path The Research and Development Agenda for Visual Analytics*, NAVC ISBN:0-7695-2323-4 https://ils.unc.edu/courses/2017_fall/inls641_001/books/RD_Agenda_VisualAnalytics.pdf.
19. Tylor and Francis (2020): *Crime Analysis and the Future* https://ebrary.net/110028/law/crime_analysis_future available on 18.11.2023.
20. UNODC (2011). *Criminal Intelligence - Manual for Analyst*, https://www.unodc.org/documents/organized-crime/Law-Enforcement/Criminal_Intelligence_for_Analysts.pdf available on 5. 11. 2023.
21. URL1: <https://www.policechiefmagazine.org/navigating-future-ai-chatgpt/> 5. 11. 2023.
22. URL2: <https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52021PC0206> available: 4. 7. 2024.
23. URL3: <https://digital-skills-jobs.europa.eu/en/actions/european-initiatives/high-level-expert-group-artificial-intelligence-ai-hleg> 5. 11. 2023.

Дилеме криминалистичко-обавештајне анализе

Апстракт: Аутори у раду истражују и истичу расност и појединачне грешке у криминалистичкој анализи коју обављају људи и вештачка интелигенција, и њихов утицај на коначни производ анализе. Такође, аутори истражују и међународну литературу о форензичкој анализи да би утврдили како се вештачка интелигенција може користити као додатак опсежној анализи података, за обављање аналитичких задатака у прикупљању доказа у виду масовних података. У форензичкој и људској анализи могу се појавити грешке, које су углавном у вези с предметом. Те грешке постоје и у анализи коју обавља вештачка интелигенција, где је ипак присутан људски рад, и то од дизајна алгоритама све до краја анализе. Актуелност теме је неупитна, јер се суочавамо са све већом количином информација чија је људска обрада потпуно немогућа.

Кључне речи: криминалистичка анализа, криминалистички аналитичари, вештачка интелигенција.