

# Network Visualization of Criminal Co-offending Patterns Using GPT-4: Analysis of Social Connections in Organized Crime\*

Olha Kovalchuk<sup>1,\*†</sup>, Serhiy Banakh<sup>1,†</sup>, Nadiya Khoma<sup>1,†</sup>, Sofia Chudyk<sup>2,†</sup>, Mariia Masonkova<sup>3,†</sup>, and Solomia Savrii<sup>1,†</sup>

<sup>1</sup> West Ukrainian National University, 11 Lvivska str., Ternopil, 46009, Ukraine

<sup>2</sup> Ukrainian Catholic University, Ilariona Svjetsits'koho St, 17, L'viv, 79000, Ukraine

<sup>3</sup> Kherson State Maritime Academy, 20 Ushakova Avenue, Kherson, 73009, Ukraine

## Abstract

Crime continues to pose a significant threat to community stability and socioeconomic development in our global society. Artificial intelligence technologies are increasingly being deployed to predict potential criminal activity and analyze the structural patterns within criminal networks through data-driven approaches. This paper introduces a novel methodology utilizing GPT-4 tools to examine social connections within criminal networks through graph-based visualization techniques. We developed a graph visualization approach for criminal data that effectively identifies structural patterns within criminal organizations. Our research analyzed 2,113 criminal cases related to vehicle theft, robberies, and armed robberies between 2013 and 2024 in the Ternopil region, resulting in visual network models of criminal co-offenders. By leveraging GPT-4's multimodal capabilities, we processed criminal data and generated graph representations illuminating the social connection structures among offenders. Our findings reveal distinctive network patterns across different crime types: vehicle theft networks demonstrate complex, highly centralized structures with key coordinator roles; robbery networks typically feature small, stable groups of 2-3 individuals, reflecting the operational requirements of such crimes; and armed robbery networks exhibit larger (4-6 person), more structured organizations with clear role distribution, likely due to the need for violence coordination and victim control. This methodology offers law enforcement agencies an effective analytical tool for addressing organized crime in contemporary settings.

## Keywords

graph-based criminal network analysis, GPT-4 network visualization, co-offending patterns, organized crime structure, law enforcement intelligence

## 1. Introduction

Crime represents an increasingly critical global challenge confronting the international community. Deteriorating economic conditions and political instability, particularly exacerbated by armed conflicts worldwide, create fertile ground for criminal activity proliferation. Military conflicts disrupt established social orders while simultaneously fostering emergent criminal behaviors. Organized criminal entities frequently develop within conflict zones, subsequently expanding their operations into neighboring territories and establishing cross-border criminal networks. These socioeconomic disruptions function as powerful accelerants for criminal environments.

Criminal activity's consequences penetrate society at multiple levels – from individuals to national institutions. Crime victims endure not only financial losses but also psychological damage and diminished personal security. At the community level, crime results in property devaluation,

---

*The Second International Conference of Young Scientists on Artificial Intelligence for Sustainable Development (YAISD), May 8-9, 2025, Ternopil, Ukraine*

\* Corresponding author.

† These authors contributed equally.

✉ o.kovalchuk@wunu.edu.ua (O. Kovalchuk); s.banakh@wunu.edu.ua (S. Banakh); n.khoma@wunu.edu.ua (N. Khoma); sophichudyk@gmail.com (S. Chudyk); masyonkova@gmail.com (M. Masonkova); solomija14@gmail.com (S. Savrii)

ORCID 0000-0001-6490-9633 (O. Kovalchuk); 0000-0002-2300-1220 (S. Banakh); 0000-0003-2981-0296 (N. Khoma); 0009-0000-8793-7258 (S. Chudyk); 0000-0001-9718-152X (M. Masonkova); 0009-0007-2352-2847 (S. Savrii)

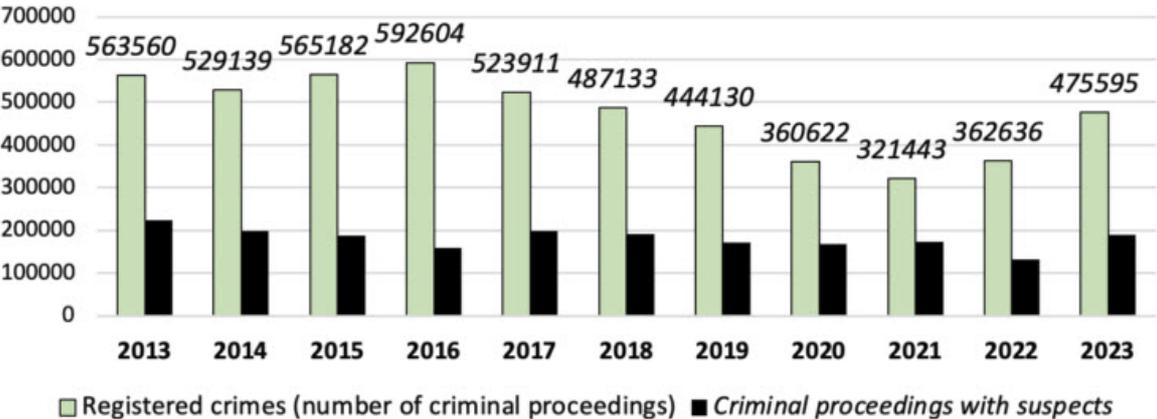


© 2025 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

heightened collective anxiety, and general degradation of living standards. On the broader societal scale, criminal activity erodes social cohesion and undermines public confidence in governmental institutions. This phenomenon manifests through diverse expressions, ranging from minor infractions to serious offenses, including violent crimes and organized criminal group operations.

The year 2024 witnessed a documented increase in global crime rates. Global statistical analyses indicate that within the past two years, approximately one in twenty individuals has experienced violent victimization [1]. Forecasts suggest an additional annual crime rate increase of 4% through 2026, driven by expanding social disparities and continued destabilization of societal structures. Regions experiencing political instability and active conflict, such as Ukraine, are projected to maintain elevated levels of violent criminal activity [2].

According to Numbeo data from mid-2024, Ukraine ranked 69th among 146 countries in the Crime Index by Country [3]. Crime in Ukraine is increasing, which can be attributed to the direct impact of martial law circumstances. However, despite the serious challenges facing the criminal justice system, crime clearance rates remain satisfactory (Fig. 1)



**Figure 1:** Registered crimes in Ukraine (2013–2023).  
Source: [4]

Crime constitutes a complex social challenge with profound implications for individuals, communities, and broader societal functioning. Developing effective prevention and response strategies necessitates implementing robust counteraction mechanisms. A particularly valuable approach involves detecting and analyzing the social connections and networks that emerge within criminal environments.

Criminal Network Analysis serves as a powerful methodology for comprehending organized crime structures and dynamics. Contemporary artificial intelligence technologies provide unprecedented capabilities for identifying concealed connections and patterns within extensive criminal datasets. AI systems can effectively process substantial volumes of unstructured information from diverse sources, ranging from police documentation to telecommunications records and social media activity. These systems can uncover hidden relationships between criminal collaborators that might remain undetectable through conventional investigative approaches. AI tools demonstrate effectiveness in predicting potential criminal conspiracies and identifying pivotal figures within criminal networks. They facilitate the creation of visual network representations that enhance investigators' understanding of criminal organizational structures. Graph Neural Networks specifically address the analysis of complex relational patterns among criminal group members. These models can identify non-intuitive structural patterns within criminal networks while predicting potential emerging connections. Developing sophisticated criminal network analysis methodologies requires interdisciplinary collaboration, integrating law enforcement expertise with advanced data analytics. Only through such comprehensive integration can truly effective tools for detecting and countering modern organized crime be established.

This article introduces an innovative approach to analyzing social connections among group crime participants through the application of GPTChart technology for criminal network modeling and visualization.

## 2. Related works

Artificial intelligence demonstrates remarkable capabilities in identifying patterns and templates within extensive datasets that would prove challenging to detect through manual examination [5]. AI has evolved into a fundamental component of contemporary forensic investigation methodologies [6]. Researchers leverage this technological capability to analyze heterogeneous criminal datasets [7-8], with particular emphasis on criminal network analysis [9]. E. Cekic investigated AI applications in developing psychological offender profiles, specifically examining its potential to uncover complex patterns of criminal behavior and underlying motivational factors [10]. J. Adkins and colleagues developed an innovative digital forensics approach that integrates multiple Natural Language Processing tools to generate potential suspect lists based on textual analysis. Their proposed methodology functions to systematically reduce large suspect pools to more focused groups of individuals demonstrating stronger connections to the investigated crime [11]. N. Shoeibi and team employed various AI methodologies to detect criminal activity on Twitter, utilizing Graph network analysis techniques to visualize user relationship structures [12]. H.V. Ribeiro and colleagues explored the application of graph convolutional networks in identifying patterns between connected criminal actors and predicting various criminal network characteristics [13]. Salcedo et al. researched Machine Learning Model applications within Criminal Networks, examining both the potential benefits and implementation challenges of advanced AI methodologies in Criminal Network Analysis [14].

Although individual studies exist in this domain, comprehensive scientific research specifically addressing AI methodologies for criminal network analysis remains relatively scarce. This paper introduces an innovative approach to analyzing criminal co-offending networks through the integrated application of graph theory principles and Chart GPT tools.

## 3. Methodology

The research implemented a multifaceted methodological approach integrating several complementary methods, including literature review, critical analysis, and case study examination, alongside the proposed application of Graph Network Analysis and ChatGPT tools for detecting and analyzing social connections within criminal co-offending networks.

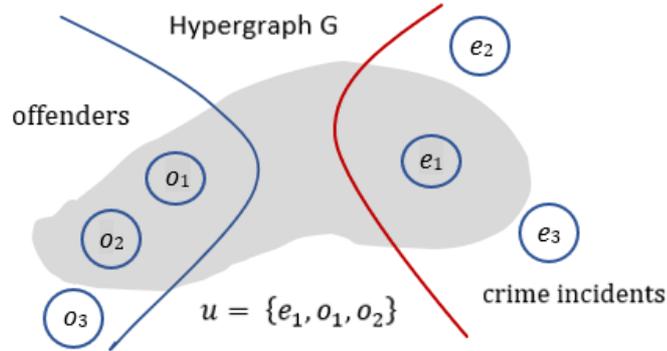
Organized crime manifests through covert groups operating through illicit channels, with significant potential to adversely impact both social structures and economic systems [15]. Criminal relationship patterns can be effectively analyzed through network theory principles, wherein these connections are categorized as covert or dark networks [16]. These networks, encompassing both terrorist organizations and criminal enterprises, can be represented mathematically as graph structures. The graph theoretical framework provides researchers with a systematic approach to examine the structural characteristics of covert networks and derive meaningful insights regarding criminal group behavioral patterns [17].

### 3.1. Suggested Model for Crime Data

Criminal data can be represented as a finite attributed bipartite hypergraph  $G$  containing  $X$  and  $U$ , which represent the vertices and edges of  $G$ . The vertex set  $X$  is divided into two mutually exclusive sets,  $O = \{o_1, o_2, \dots, o_p\}$ ,  $E = \{e_1, e_2, \dots, e_q\}$ , reflecting offenders and events referring to crime incidents of a certain type.

The set  $U$  consists of hyperedges such that each  $e \in U$  is a subset of vertices  $\{u_1, u_2, \dots, u_n\} \subseteq U$  with  $|u \cap E| = 1$  (each edge is connected to exactly one incident) and with  $|u \cap O| \geq 1$  (at least one offender).

For any  $u, u' \in U$  with  $u \cap E = u' \cap E$  it follows that  $u = u'$ . It means that every edge  $u$  of  $G$  identifies a subset of offenders  $o_{e_1}, o_{e_2}, \dots, o_{e_j}$  with any crime event  $e_k \in E$ , that is  $= \{e_k, o_{e_1}, o_{e_2}, \dots, o_{e_j}\}$ . An example is shown in Figure 2.



**Figure 2:** Crime data model hyperedge.

he suggested model does not consider the frequency of repeat offenses committed by the same pair of accomplices. In the context of martial law, criminal networks are highly volatile. Our objective is to uncover the presence of social ties between the offenders and assess the size of criminal groups.

### 3.2. GPT-Based Chart for Graph Network

GPT-4 comes with built-in features for creating and visualizing graphic elements, including the ability to generate graphs of various complexities. The system can create structured graph representations where nodes, edges, and their attributes can be defined. A key feature is the ability to customize the visual style of graph elements, such as size, color, shape, and connection line types.

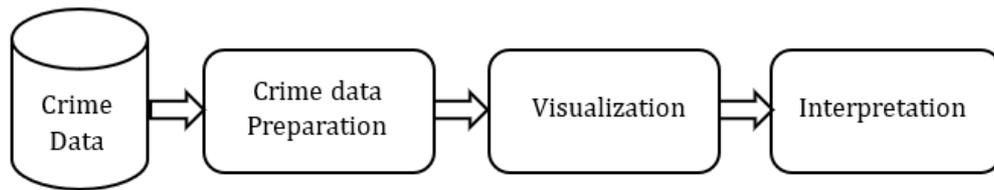
When working with graphs, GPT-4 enables the creation of both simple tree structures and intricate network diagrams with different connection types between nodes. It supports multiple visualization formats, such as directed and undirected graphs, weighted graphs, and hierarchical structures. Additionally, element positioning, labels, and legends can be customized to enhance understanding of the data. These capabilities make GPT-4 a powerful tool for visualizing complex relationships across various domains, from social network analysis to depicting organizational structures and business processes.

We used GPT-4 tools to visualize complex network structures to streamline the analysis of criminal groups. Our goal was to generate structured graph representations with the following elements:

- nodes (or vertices) represent individual participants in criminal activity;
- edges (or links) of a graph (or network) show connections between the offenders (nodes).

### 3.3. Proposed approach

This study presents a novel methodology for detecting and analyzing criminal networks using Graph Network Analysis by the ChatGPT tool (Figure 3).



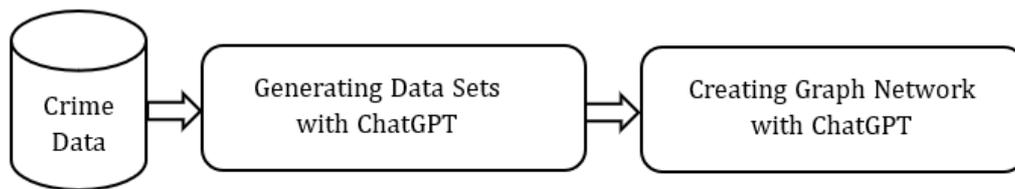
**Figure 3:** Flow chart of the proposed approach for analysis of social connections within criminal co-offenders.

Our dataset was developed from crime data through natural language generation processes utilizing GPT-4 [18]. Through this advanced AI tool, we transformed factual criminal case information into a structured table containing essential elements for criminal network graph construction: comprehensive data regarding individual perpetrators, detailed classification of crime types committed, and specific information about co-offending relationships [19].

We employed the sophisticated large multimodal model GPT-4 to construct graphical representations that visually depict the social connection networks existing between criminals who participated in collaborative criminal activities [20]. These visual graph structures effectively illuminate the relationship patterns and organizational structures within criminal co-offending networks.

### 3.4. Data selection and description

To detect and analyze criminal networks, we utilized data on actual crimes committed between 2013 and 2024 in the Ternopil region of Ukraine. With the help of ChatGPT-4, we generated datasets from 2,113 criminal cases involving vehicle theft, robberies, and larceny. These datasets contain information about the offenders and the criminal incidents associated with these offenses. Using the generated datasets, we constructed graphs illustrating the social connections within criminal networks through GPT-4. The edges of the graph represent links between criminals who committed crimes as part of the same group. The connections between offenders are indicated by the graph's edges, showing those who committed crimes together. The steps of dataset generation and graph network creation are depicted in Figure 4.



**Figure 4:** Generating data sets and creating a graph network process

Input Data Set records contain information about crimes committed by each perpetrator and have the following attributes:

- offender;
- crime identifier;
- date of crime;
- settlement where the crime was committed;
- location of the incident;
- time of incident;
- lighting;
- crime committed in a group;
- type of crime;
- day of the week;

- area/locality.

For the generation Data Set, which was used to create co-offender network graphs, we used ChatGPT-4. Using the prompt "Based on the given table, generate a new table with the following attributes: crime identifier, offender, type of crime", a new table was created. If a crime was committed with accomplices, for one crime identifier, it contains several records with different values of the "offender" attribute. Based on the newly created table, ChatGPT-4 built co-offender graphs for each of the analyzed types of crimes: illegal appropriation of a vehicle, theft, and robbery. Figure 4 illustrates the workflow beginning with raw crime data, the formation of a new data table containing the necessary attributes for a graphical representation of the criminal network, and the creation of a co-offender graph. Its vertices represent criminals from the dataset; edges visualize social connections between them (indicating the presence of crimes committed jointly by the corresponding pair of offenders).

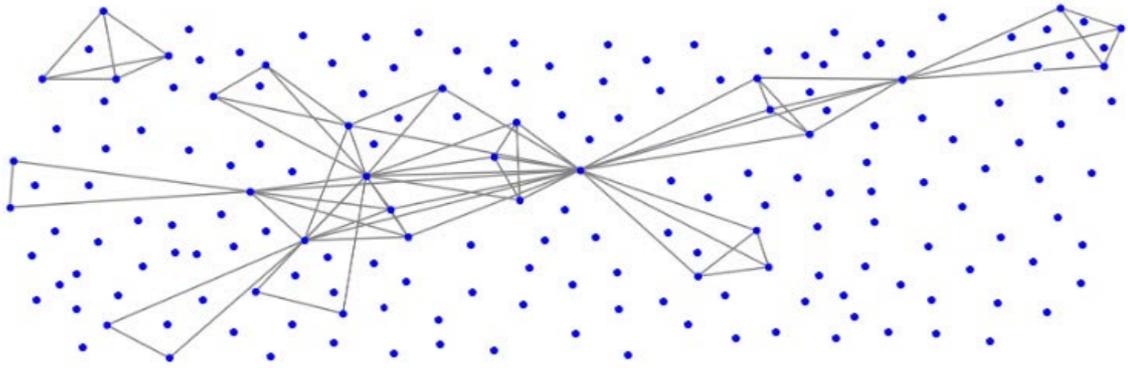
## 4. Results and discussion

Visualization can support the examination of social ties within criminal networks. It helps uncover interaction patterns among offenders, recognize criminal groups, identify key organizers and their roles, and reveal communication structures between individuals involved [20–21]. The visualization of offender networks extends beyond mere image creation, offering potential for more in-depth investigation and analysis of criminal relationships.

Utilizing data from 2,113 actual criminal cases, including perpetrator and offense information, we developed criminal network visualizations with ChatGPT technology. Separate visual models were created for three crime categories (vehicle theft, general theft, and robbery) committed within Ukraine's Ternopil region from 2013 to 2024. The multimodal GPT-4 system helped transform raw crime data into structured tables containing essential attributes for visualizing criminal relationships [19]. This processed information was then used to generate graphs depicting the network of criminal associations using GPT-4 [20].

Figure 5 displays a network graph illustrating interactions among vehicle theft offenders. In this visualization, nodes represent individual criminals while connecting lines indicate co-participation in crimes. Our analysis focused on identifying network structure patterns. The graph construction considered the presence of criminal partnerships but not the frequency of repeated offenses within groups. This visual representation reveals extensive interconnections between offenders and suggests unstable criminal group dynamics, evidenced by numerous cross-connections between different network participants.

Notably, nodes with high centrality point to key individuals within the network who maintain numerous connections with others, potentially serving as organizers or coordinators of criminal operations. Additionally, the presence of tightly connected clusters suggests established criminal groups, possibly specializing in vehicle theft. This is supported by the fact that professional car thefts are often carried out by organized groups of 2–3 to 5–6 individuals, each fulfilling a specific role, such as thief, driver, or reseller. Such a structure is essential due to the complexity of modern car security systems and the logistical demands of quickly concealing stolen vehicles [23].

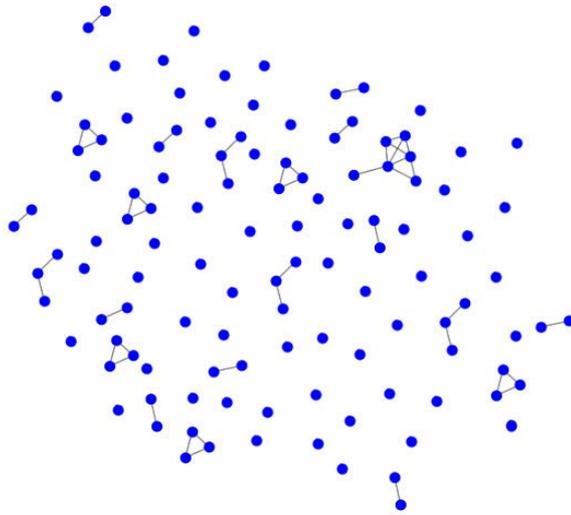


**Figure 5:** Visual model of co-offenders of illegal appropriation of a vehicle.

Individuals who committed vehicle theft alone are depicted as isolated nodes in the graph. These instances are typically associated with opportunistic thefts, such as when a vehicle is left with keys in the ignition, older cars with less advanced security systems, or joyriding. The high number of isolated nodes suggests that many offenders acted without accomplices. This trend may be attributed to the dataset covering three years of martial law in Ukraine, during which the structure of criminal activity changed significantly, and many connections were disrupted. Additionally, increased social vulnerability and large-scale population displacement played a role. Despite this, the visual model of social interactions among vehicle theft offenders still reveals the presence of extensive criminal networks. However, determining the precise proportion of group versus solo thefts remains challenging due to a significant number of unsolved cases.

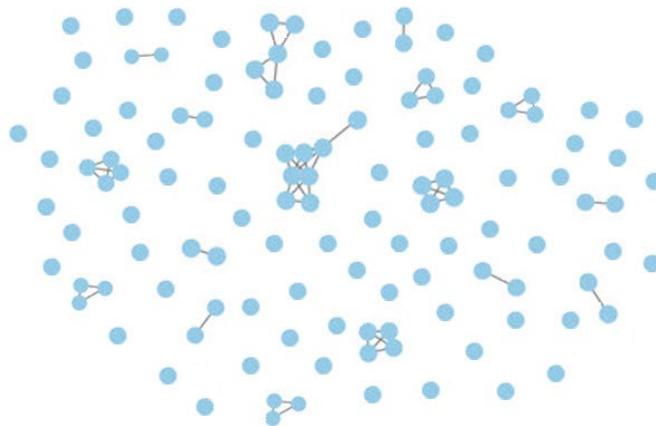
Figure 6 presents a visual model of criminal interactions among individuals involved in robberies. The number of offenders committing this type of crime is notably lower compared to those involved in vehicle appropriation. Robberies are typically carried out by small groups of 2–3 individuals, particularly in cases involving attacks on pedestrians at night, public space robberies, assaults on cash couriers or banks, and store hold-ups. Group assaults are more effective as they allow better control over the situation and the victim, improve chances of overcoming resistance, and enable role division, such as one offender threatening while another seizes valuables [24]. These groups tend to be relatively stable, as successful robberies require coordinated action, mutual trust, and a clear understanding of each participant’s role. Graph analysis reveals that a substantial portion of the nodes are linked in stable 2–3-member components, supporting the pattern of forming small, consistent criminal groups for robbery offenses. Methods of presenting information in web format are given in the work [25]. Approaches to data analysis using AI are presented in the works [26–27].

Individual robberies are more commonly associated with assaults on elderly victims, impulsive and unplanned acts, offenses committed under the influence of alcohol or drugs, and minor street crimes such as bag or phone snatching. The large number of isolated nodes in the graph depicting robbery-related interactions suggests a considerable share of situational and uncoordinated crimes within the broader robbery landscape. This pattern indicates that many of these offenses occur spontaneously, without prior planning, and are not linked to organized criminal networks.



**Figure 6:** Visual model of co-offenders of thefts.

Figure 7 illustrates a visual representation of criminal interactions among individuals involved in robberies. The graph of co-offenders in this crime category reveals well-defined criminal groups, which appear more frequently than in theft-related cases. This is primarily due to the nature of robbery, which is commonly carried out by groups. Group robberies are particularly prevalent in incidents such as home invasions, business or store robberies, attacks on cash couriers, and highway heists. The dominance of group involvement can be attributed to the necessity of using or threatening violence, managing multiple victims at once, increasing the chances of overcoming resistance, and ensuring a swift escape and transportation of stolen items.



**Figure 7:** Visual model of co-offenders of robbery.

The graph depicted in Figure 7 includes a notable number of isolated nodes, representing offenders who carried out robberies individually. Such incidents typically involve attacks on lone pedestrians, impulsive and unplanned crimes, assaults in sparsely populated areas, or offenses committed by repeat offenders. In contrast to thefts, robberies exhibit more distinctly organized criminal groups and a greater density of connections between co-offenders [28–29]. The visual model highlights the coexistence of both large, structured criminal groups and a substantial number of solo perpetrators. During the period of martial law, the structure of robbery-related crime has shifted significantly. There has been a rise in armed robberies, particularly involving weapons obtained from combat zones. Additionally, there is a growing trend of robberies targeting the homes of internally displaced persons and temporarily abandoned properties near conflict areas. A notable development

is the emergence of criminal groups composed of former military personnel, who apply the skills and knowledge acquired through their service.

The analysis of visual models representing criminal networks for three crime categories (illegal vehicle appropriation, thefts, and robberies) reveals notable differences in the structure of criminal interactions and group formation patterns. The visual representation of network data enabled the identification of distinct organizational patterns in criminal activities, ranging from complex interconnected networks in vehicle theft to more organized group structures in robberies. A key advantage is the ability to pinpoint central figures and stable criminal groups, which is of vital importance for law enforcement agencies. The impact of martial law on the crime landscape is evident, with a rise in isolated offenders and the emergence of new forms of group criminal behavior. High-quality visualization and interpretation of the data bridge the gap between theoretical analysis of criminal networks and practical law enforcement efforts, offering an effective tool for understanding and combating organized crime in contemporary contexts.

## 5. Conclusions

The article introduces an innovative method for analyzing social connections within criminal networks by utilizing GPT-4 tools for data visualization and interpretation. A new methodology was developed to represent criminal data as a finite, attributed bipartite hypergraph and to create visual models of criminal interactions based on this representation. Using data from 2,113 criminal cases involving vehicle theft, robberies, and larcenies committed in the Ternopil region between 2013 and 2024, co-offender network graphs for these crimes were generated and analyzed. By applying the GPT-4 multimodal model, unstructured data from criminal cases was processed to create a structured table with the necessary attributes for visualization. With this data, and utilizing ChatGPT tools, graphs were constructed to illustrate the social connections between criminals, where vertices represent individual offenders and edges depict instances of their criminal collaboration.

The research conducted highlights the effectiveness of using GPT-4 tools for analyzing and visualizing social connections within criminal networks. By applying the proposed methodology to real crime data, significant variations in the structure of criminal interactions were observed across different types of crimes.

Visual models revealed that vehicle theft is associated with complex, interconnected networks and key figures with a high degree of centralization. Robberies tend to involve smaller, more cohesive groups of 2-3 individuals, while armed robberies are characterized by the formation of larger, more organized criminal groups. Notably, a significant number of isolated individuals were identified across all crime types, which could be linked to the destabilization of the criminal environment due to martial law conditions.

The visual representation of network data offers investigators valuable insights into the structural characteristics of criminal groups, especially under martial law conditions. The proposed methodology, which integrates GPT-4's capabilities for data processing and visualization, provides a powerful tool for analyzing criminal networks. High-quality visualizations and detailed interpretation of the results help bridge the gap between theoretical analysis and practical law enforcement efforts, offering effective means for understanding and combating organized crime in contemporary settings. Future research will focus on enhancing algorithms for detecting hidden connections and predicting potential criminal conspiracies, employing more advanced graph analysis techniques and machine learning methods. Specifically, the issue of repeat offenses by established criminal groups will be explored.

## Acknowledgments

The authors express their sincere gratitude to the Armed Forces of Ukraine for providing security, which made it possible to conduct our research.

## Declaration on Generative AI

During the preparation of this work, the authors used GPT-4 tools to generate a dataset from the input table and to visualize complex network structures to simplify the analysis of criminal groups. All processes are described in the research methodology. After using these tools, the authors reviewed and edited the content as needed and took full responsibility for the publication's content.

## References

- [1] The Global Safety Report. Gallup. 2024. URL: [https://insightcrime.org/wp-content/uploads/2024/10/Gallup\\_Global-Safety-Report-2024.pdf](https://insightcrime.org/wp-content/uploads/2024/10/Gallup_Global-Safety-Report-2024.pdf).
- [2] Joshi K. Crime Statistics by Country Crime Index and Facts. 2024. URL: <https://www.coolest-gadgets.com/crime-statistics/>.
- [3] Crime Index by Country 2024 Mid-Year. Numbeo. URL: [https://www.numbeo.com/crime/rankings\\_by\\_country.jsp](https://www.numbeo.com/crime/rankings_by_country.jsp).
- [4] D. Yagunov, The Ukrainian Prison and Probation Policy (1991 – 2024): Modulations and Key Indicators. *Evropský časopis ekonomiky a management* 10(4) (2024) 17–86. doi:10.46340/eujem.2024.10.4.2.
- [5] J.P. Bharadiya. Machine learning and AI in business intelligence: Trends and opportunities. *Int. J. Comput.* 48(1) (2023) 123–134.
- [6] A. Jarrett, K.K.R. Choo. The impact of automation and artificial intelligence on digital forensics. *Wiley Interdiscip. Rev. Forensic Sci.* 3(6):e1418 (2021). doi:10.1002/wfs2.1418.
- [7] P. Sarzaeim, Q.H. Mahmoud, A. Azim, G. Bauer, I. Bowles. A Systematic Review of Using Machine Learning and Natural Language Processing in Smart Policing. *Computers* 12(12):255 (2023). doi:10.3390/computers12120255.
- [8] C. Rigano. Using Artificial Intelligence to Address Criminal Justice Needs. *National Institute of Justice. NIJ Journal* 280 (2019).
- [9] A. Ficara, F. Curreri, G. Fiumara, P. De Meo, A. Liotta. Covert Network Construction, Disruption, and Resilience: A Survey. *Mathematics* 10(16):2929 (2022). doi:10.3390/math10162929.
- [10] E. Cekic. The Impact of Artificial Intelligence Tools on Criminal Psychological Profiling. *International Journal of Academic Research in Psychology* 11(1) (2024) 1–13. doi:10.46886/IJARP/v11-i1/7405.
- [11] J. Adkins, A.A. Bataineh, M. Khalaf. Identifying Persons of Interest in Digital Forensics Using NLP-Based AI. *Future Internet* 16(11):426 (2024). doi:10.3390/fi16110426.
- [12] N. Shoeibi, N. Shoeibi, G. Hernández, P. Chamoso, J.M. Corchado. AI-Crime Hunter: An AI Mixture of Experts for Crime Discovery on Twitter. *Electronics* 10(24):3081 (2021). doi:10.3390/electronics10243081.
- [13] H.V. Ribeiro, D.D. Lopes, A.A.B. Pessa, A.F. Martins, B.R. da Cunha, S. Gonçalves, E.K. Lenzi, Q.S. Hanley, M. Perc. Deep learning criminal networks. *Chaos, Solitons & Fractals* 172:113579 (2023). doi:10.1016/j.chaos.2023.113579.
- [14] E. Salcedo-Albarán, L.J.G. Salamanca, J.A. Cano-Melani. Machine Learning Models on Criminal Networks (MLMoCN): Artificial Intelligence to Disentangle Crime. *SSRN Electronic Journal* (2023). doi:10.2139/ssrn.4651714.
- [15] O. Kovalchuk, M. Shynkaryk and M. Masonkova. Econometric Models for Estimating the Financial Effect of Cybercrimes, in: *Proceedings of the 11th International Conference on Advanced Computer Information Technologies*, Deggendorf, Germany, 2021, pp. 381–384. doi: 10.1109/ACIT52158.2021.9548490.
- [16] O. Kovalchuk, M. Masonkova and S. Banakh. The Dark Web Worldwide 2020: Anonymous vs Safety, in: *Proceedings of the 11th International Conference on Advanced Computer Information Technologies*, Deggendorf, Germany, 2021, pp. 526–530. doi:10.1109/ACIT52158.2021.9548578.
- [17] A. Ficara, R. Saitta, G. Fiumara, P. de Meo, A. Liotta. A Game of Thieves and WERW-Kpath: Two Novel Measures of Node and Edge Centrality for Mafia Networks. In *Complex Networks XII*, Springer International Publishing: Cham, Switzerland, 2021, pp. 12–23. doi:10.1007/978-3-030-81854-8\_2

- [18] O. Kovalchuk, R. Shevchuk, M. Masonkova, A. Banakh. Content Analysis of Court Decisions: A GPT-4 Based Sentence-by-Sentence Data Generation and Association Rules Mining, in: Proceedings of the I International Workshop of Young Scientists on Artificial Intelligence for Sustainable Development 2024, pp. 56-70. URL: <https://ceur-ws.org/Vol-3716/paper5.pdf>.
- [19] D. Gewirtz. How to use ChatGPT's Advanced Data Analysis to create quality charts and tables. URL: <https://www.zdnet.com/article/how-to-use-chatgpt-to-make-charts-and-tables-with-advanced-data-analysis/>.
- [20] S. Lanoue. How to Use ChatGPT to Make Charts and Graphs. URL: <https://www.thebricks.com/resources/how-to-use-chatgpt-to-make-charts-and-graphs>.
- [21] E.K. Anastasiadis, I. Antoniou. Directed Criminal Networks: Temporal Analysis and Disruption. *Information* 15(2):84 (2024). doi:10.3390/info15020084.
- [22] K. Zhao, H. Zhang, J. Li, Q. Pan, L. Lai, Y. Nie, Z. Zhang. Social Network Forensics Analysis Model Based on Network Representation Learning. *Entropy* 26(7):579 (2024). doi:10.3390/e26070579.
- [23] A. Quinn Vehicle Crime, CPTED, and Offending under the Influence: A Qualitative Investigation of Offender Perceptions. *Social Sciences* 8(3):88 (2019). doi:10.3390/socsci8030088.
- [24] E. Kwon, S. Jung, J. Lee. Artificial Neural Network Model Development to Predict Theft Types in Consideration of Environmental Factors. *ISPRS International Journal of Geo-Information* 10(2):99 (2021). doi:10.3390/ijgi10020099.
- [25] M. Dyvak, A. Kovbasityi, A. Melnyk, I. Shcherbiak and O. Huhul, "Recognition of Relevance of Web Resource Content Based on Analysis of Semantic Components," 2019 9th International Conference on Advanced Computer Information Technologies (ACIT), Ceske Budejovice, Czech Republic, 2019, pp. 297-302, doi: 10.1109/ACITT.2019.8779897.
- [26] H. Zhang, Y. Gao, D. Yao, J. Zhang. Interaction of Crime Risk across Crime Types in Hotspot Areas. *ISPRS International Journal of Geo-Information* 12(4):176 (2023). doi:10.3390/ijgi12040176.
- [27] Bezobrazov, S., Sachenko, A., Komar, M., & Rubanau, V. (2016). THE METHODS OF ARTIFICIAL INTELLIGENCE FOR MALICIOUS APPLICATIONS DETECTION IN ANDROID OS. *International Journal of Computing*, 15(3), 184-190. <https://doi.org/10.47839/ijc.15.3.851>
- [28] N. Ocheretnyuk, M. Dyvak, T. Dyvak and I. Voytyuk, "Structure identification of interval difference operator for control the production process of drywall," 2013 12th International Conference on the Experience of Designing and Application of CAD Systems in Microelectronics (CADSM), Lviv, Ukraine, 2013, pp. 262-264.
- [29] M. Rasmusson, V. Helbich. The Relationship between Near-Repeat Street Robbery and the Environment: Evidence from Malmö, Sweden. *ISPRS International Journal of Geo-Information* 9(4):188 (2020). Doi:10.3390/ijgi9040188.
- [30] Lytvyn, V., Vysotska, V., Shatskykh, V., Kohut, I., Petruchenko, O., Dzyubyk, L., Bobrivetc, V., Panasyuk, V., Sachenko, S., & Komar, M. (2019). Design of a recommendation system based on collaborative filtering and machine learning considering personal needs of the user. *Eastern-European Journal of Enterprise Technologies*, 4(2 (100), 6-28. <https://doi.org/10.15587/1729-4061.2019.175507>