Journal of Namibian Studies, 33 S3(2023): 2820–2841 ISSN: 2197-5523 (online)

Security Forecasting for Detecting Organized Crimes: New Strategies and Trends

Ehab M A Alrousan[1], Raed S.A Faqir[2]

[1]Associate Prof in Criminal Law, College of Law, American University in the Emirates (AUE), UAE

[2]Associate Prof in Criminal Law, College of Law, American University in the Emirates (AUE), UAE

Associate Prof in Criminal Law, Faculty of Law, Al- Balqa' Applied University (BAU), Jordan

Abstract

The study on "Security Forecasting for Detecting Organized Crimes" aims to explore the opportunities and challenges associated with detecting future crimes, particularly organized crimes and cybercrimes. The study examines various models for understanding organized crimes and identifies new strategies that can be implemented to combat them. The research methodology involves analyzing and critically studying existing security forecasting strategies and approaches used for detecting potential organized crimes, terrorism, human trafficking, and money laundering. The study also explores the impact of new technologies on these areas and the contemporary trends in preventing potential organized crimes. The research relies on secondary sources, such as books, case law reviews, statutes, international treaties, articles, and journals, and involves conducting intensive library research and using internet searches. The study concludes that security forecasting is crucial for detecting organized crimes and preserving security for individuals and societies. The study recommends the use of security surveillance and criminal analysis technologies, availability of sufficient resources, privacy and security standards, and enhanced cooperation, exchange of information, and sharing of experiences in the field of combating organized crime. Overall, the study highlights the importance of proactive measures and continuous improvement in the field of security forecasting for detecting organized crimes.

Keywords: Security Forecasting, Detecting, Organized Crimes, Models, Strategies, New Technologies, Proactive Measures.

1. Introduction

Security forecasting is considered one of the most important methods used to detect future crimes. This type of forecasting involves using advanced technologies and big data to analyze patterns and trends in potential security risks and crimes. The concept of security forecasting relies on the assumption that current crimes and security events provide evidence of what might happen in the future. This means that future crimes and events can be anticipated based on the analysis of current patterns and trends. To achieve this goal, security forecasting uses a range of techniques such as big data analysis, machine learning, artificial intelligence, statistical analysis, geographic analysis, behavior analysis, temporal analysis, and psychological analysis. Security forecasting is applied in various fields such as cyber security, public security, national security, internal security, aviation security, border security, and industrial security. Although security forecasting can be effective in detecting future crimes, it is important to consider many potential factors that may affect the accuracy of predictions, such as social, political, economic, and technological changes, as well as changes in natural circumstances.

Security forecasting provides many benefits when it comes to detecting organized crime and cybercrime, including: firstly, improving the ability to predict future crimes: Security surveillance can analyze current patterns and trends of organized crime and cybercrime to improve the ability to predict future crimes, thereby enabling better preventive measures and prioritization. Secondly, enhancing cybersecurity: Security surveillance can use analysis and machine learning techniques to analyze cyber activity data, identify potential malicious activities, and pinpoint weaknesses in cybersecurity systems, thus improving cybersecurity and preventing cyber-attacks. Thirdly, increasing resource efficiency: Security surveillance can help improve the efficient use of resources by identifying priorities and areas that require greater focus, thereby directing resources more effectively to achieve maximum effectiveness. Fourthly, improving investigation capabilities: Security surveillance can improve the ability to investigate organized crime and cybercrime by using geographic analysis, behavioral analysis, and psychological analysis to identify suspects and analyze available evidence to provide more accurate and data-driven evidence.

Security intelligence works to combat terrorism, human trafficking, money laundering, organized and cybercrime by collecting and analyzing information and monitoring suspicious activities. Investigators and analysts gather information from multiple sources such as police, intelligence services, government agencies, private sector, and civil society organizations. This information is analyzed and reports are prepared on suspicious and suspected activities. Additionally, security agencies use modern technology to monitor suspicious activities online and track cybercrime. Analysis and prediction tools are used to identify

areas that may experience possible crimes and to determine preventive efforts that can be taken to prevent them. To protect the security and stability of society, security agencies must work to enhance cooperation and coordination with partners in government, private sector, and civil society organizations. Awareness and education must be enhanced to increase awareness of crimes and security risks and to promote preventive measures.

Public security and stability cannot be achieved without effectively and strictly enforcing the law against those responsible for security crimes. Legal sanctions must be strong and appropriate for the crimes committed, and must be applied fairly and immediately to the accused. There must be cooperation between the different entities involved in crime prevention, including the police, judiciary, intelligence services, customs, civil society organizations, and other partners. Multiple-level strategies must also be implemented to combat crime and ensure that all entities involved participate in preventive, investigative, and enforcement efforts. Awareness and education about security crimes and potential risks must be enhanced, and cooperation among partners must be encouraged to improve responses to security threats. In general, security agencies must have a strong ability to deal with various security challenges and adopt new and innovative methods to confront and combat crime, such as the use of technology.

2. Research Problem

The world of crime is constantly evolving, and law enforcement agencies face a daunting task of predicting and preventing future crimes. This is due to the rapid advancement of technology, which has enabled criminals to use sophisticated techniques to evade detection. Additionally, criminal behavior is constantly changing, and accurate data and predictive models are often lacking, making it difficult to identify potential threats. Traditional methods of detecting and preventing organized crime have proven to be inadequate, leading to the development of new models for understanding it and planning for new strategies to combat it. Organized crime is a complex and sophisticated phenomenon that operates in various forms and across different geographical regions. Therefore, a comprehensive model is essential for effective prevention and detection.

Cybercrime has emerged as a new frontier in the criminal landscape, requiring novel approaches to prevent and counter it. This involves the development of robust cybersecurity systems and the enactment of stringent laws. It is a multi-faceted problem that requires collaboration between various stakeholders, including law enforcement agencies and technology experts. In summary, the research problem is the need to detect and prevent future crimes, the inadequacy of traditional methods to combat organized crime, and the need for novel approaches to

prevent and counter cybercrime. The solution lies in developing new models for understanding organized crime, planning for new strategies to combat it, and the development of contemporary security techniques that incorporate the latest technologies and methods.

3. Literature Review Method

The current research methodology is doctrinal, meaning it focuses on legal propositions and doctrines. The methodology involves analyzing and critically studying strategies and approaches used for security forecasting. This includes detecting potential organized crime, cybercrime, terrorism, human trafficking, and money laundering. The study also explores how new technologies affect these areas. The research relies on secondary sources, such as books, case law reviews, statutes, international treaties, articles, and journals. Material collection will involve conducting intensive library research and using internet searches.

4. Results and Discussions

4.1: What are the opportunities for future Crimes?

Theoretical perspectives endeavor to elucidate the nature and mechanics of organized crime. Consequently, these perspectives furnish proof of the elements comprising "opportunity" for organized crime and the avenues that criminal syndicates can exploit. However, automated theories have revolutionized evaluations of organized crime. Therefore, appraisals of organized crime can no longer furnish information about the potentialities for criminal groups to exploit or the level of certainty concerning such opportunities. Before addressing this question, it is imperative to establish that the crimes committed represent merely one facet of organized crime. In this form of criminal activity, groups exploit a diverse array of environmental opportunities and conditions, executing offenses in a fluid manner that relies on sophisticated scientific and technical methodologies. These crimes often span a wide-ranging and expansive scope, with the crime scene extending outward from its core. Institutional involvement may appear to operate individually or as part of a legitimate coalition. This affords criminals a distinct advantage.

The answer to this question depends heavily on the theoretical perspective applied to the particular type of crime being discussed. Crimes that are categorized as unique, such as white-collar crimes, cybercrimes, and organized crimes, differ significantly from ordinary crimes in terms of their fundamental nature, concept, means and conditions of commission, as well as the opportunities they present for criminal activity. Under what circumstances does the ability to predict future crimes vary between different types of criminal activities? Crime

occurrences are closely correlated with changes in security data and the effectiveness of security institutions in a locality. The company's authority must evaluate the projected results, taking into account unreported shadow crimes, particularly offered offenses, as well as external factors such as political, social, cultural, economic, environmental, and legal variables.

4.2: Challenges and Difficulties for Detecting Future Crimes

While it may be challenging for security services to detect and prevent future crimes, it is crucial that we take action to protect society from the most serious organized crimes. These crimes can have far-reaching consequences that can impact the safety and well-being of individuals and communities. It is important to recognize that social and criminal phenomena are not bound by their past or present circumstances alone. Rather, they are also influenced by future events and changes in social and natural laws (Wortley & Townsley, 2017. 98-99). This means that our actions today can have a significant impact on shaping the future of crime and society as a whole. Therefore, it is imperative that we take a proactive approach to addressing organized crime, and invest in effective prevention and intervention strategies. By doing so, we can create a safer and more secure future for everyone.

When we talk about the future, we're referring to time periods that haven't happened yet. To understand what's to come, we must consider how humanity has progressed through the past, present, and future. The present is shaped by events and experiences of the past, and the future is similarly influenced by the current and past realities, circumstances, and factors. Essentially, the future is seen as an extension of the past and present, and by analyzing current events and their impact, we can make predictions about what's to come (Arendt, 1961, Pp.5,6,10). By interpreting and analyzing present-day events and their implications, we can gain valuable insight into what we can expect in the future.

The concept of future justice is centered around the police, security services, and their associates, with the ultimate goal of creating a safer society. It involves leveraging present-day techniques and resources to prevent the occurrence of future crimes. With the help of technology-based planning and monitoring methods, security agencies can potentially predict and analyze criminal behavior, particularly in relation to high-harm crimes like terrorism, cybercrime, money laundering, extortion, and others. The proactive approach of future justice is crucial in mitigating the widespread impact of such crimes and ensuring the safety of society as a whole.

Al-Hindawi and Al-Hamouri cautioned in their book "Future Foresight & Shaping" about the misconception that change is governed by an unchanging law. Today's security institutions require proactive decisions based on data that is converted into actionable information (Al-Hindawi and Others, 2017, p. 40). According to Hindawi, while the future may be

uncertain, it can be predicted by specific events and information. Additionally, history repeats itself through recurring phenomena, and we must learn from it to look forward to the future. Historical predictions cannot be made in isolation from the laws of change, such as (Moore's Law, Feller's Law for Accelerated Knowledge), which reveal patterns or trends underlying the development of social and criminal phenomena (Hindawi and others, 2017, p. 25, 40, 56).

Kilani (1986) argues that history is an objective reality with an inevitable end, which shapes the goals that define our future. What we do in the past will affect the future, and modern societies always link their future to their past and present. History is close and incriminating, yet invaluable and ultimately a result of human decision-making (El Kilani, 1986, P.32-35, pp. 34-35). Therefore, all our current actions, decisions, writings, and perceptions are linked to an uncertain future. As a result, modern societies fear future developments and changes that may pose risks and threats to community peace and security. This fear prompts state institutions, particularly security institutions, to take proactive action to confront any emergency that may threaten the future peace and security of the community.

To effectively anticipate and prevent organized crime, relying solely on old prediction models or possibilities is unlikely to be successful. Rather, it requires a proactive approach by security authorities, based on the results of a security forecast, which enables police and judicial control authorities to make decisions aimed at preventing crime. It's important to keep in mind that prediction results may be uncertain, as they are linked to an uncertain future. Currently, the future of organized crime is posing greater risks and threats, particularly with the acceleration of digitization, increased connectivity, and significant increases in data. Our understanding of this future is constantly evolving, as different areas such as smart materials, biotechnology, and artificial intelligence converge and erase boundaries between physical, digital, and biological spaces. This creates more uncertainty and challenges for security and policing. In light of these developments, future crime prediction models need to be reviewed and updated, taking into account accelerated scientific and technological advancements. Additionally, the concept of organized crime needs to be redefined in terms of its concept and substance.

The topic of organized crime is complex and multifaceted, encompassing various forms, dimensions, challenges, risks, and threats. Our understanding of this serious criminal phenomenon is closely linked to how we perceive it today. Unfortunately, in recent years, organized crime has emerged as a major threat to safety and justice systems worldwide. The rapid advancement of technology has allowed criminal organizations to adapt and evolve, changing the way we view organized crime. As a result, our knowledge base on organized crime has expanded to include new forms of criminal activity, such as organized cybercrime,

money laundering, white-collar crime, and human trafficking. Additionally, the rise of organized terrorism has further complicated the issue (Najmuddin, 2021, 93). In summary, the future of organized crime is a topic of great concern, and it is important that we continue to study and understand this phenomenon to effectively combat it.

4.3: Models of Understanding Organized Crimes

It's important to note that organized crime has evolved significantly over time. In the past, the concepts and practices associated with it were different from what we see today. Currently, we are witnessing further developments in this area, with transnational organized crime organizations forming alliances with terrorist groups. This has led to a shift from a "bureaucratic model" to a more complex "web model" of organized criminality, with the emergence of third-generation gangs. Unlike first and second-generation gangs, these groups are not solely focused on opportunistic crimes within national borders. Instead, they pursue their goals through internationalization, technical development, and politicization. They seek not only financial gain, but also economic and political control (Maouqbel, 2018, p. 117-118). Today, trans-border criminal organizations engage in a variety of illegal activities that cannot be accurately measured or quantified. They form alliances and deals with other parties, including terrorist groups (Maouqbel, 2018, p. 113). Therefore, their activities go beyond just commercial endeavors.

The "hierarchical model" is different from the "patron-client model" and the "enterprise model" when it comes to organized crime. This model views the mafia as a bureaucratic organization within the State. The main difference between the three models lies in how they view the leadership of the criminal organization (Lampe, 2003). The "patron-client model" shows organized crime as a network of asymmetric links within ethnic or local networks. On the other hand, the "enterprise model" interprets organized crime as an economic activity. These models reveal different mechanisms for how organized crime operates. The differences between the three models of organized crime can be summarized as following:

• Hierarchical model: This model views the mafia as a bureaucratic organization within the state. It suggests that the mafia operates like a legitimate business, with clear lines of authority and a hierarchy of power. For example, the Sicilian Mafia is often cited as an example of a hierarchical criminal organization. The boss, or "capo di tutti capi", is at the top of the hierarchy, followed by underbosses, captains, soldiers, and associates. Each level has a specific role to play, and members must follow a strict code of conduct.

• Patron-client model: This model sees organized crime as a network of asymmetric links within ethnic or local networks. It suggests that criminal organizations are formed through personal relationships and mutual obligations, rather than a formal hierarchy. For example, in the

case of the Japanese Yakuza, members are bound together by a sense of loyalty to their boss (oyabun) and their fellow members (kobun). This loyalty is based on the concept of "giri", or obligation, which requires members to repay favors and protect the group's interests.

• Enterprise model: This model views organized crime as a form of economic activity. It suggests that criminal organizations are motivated by profit, rather than traditional criminal goals such as power or revenge. For example, the Colombian drug cartels are often cited as an example of an enterprise-based criminal organization. These cartels are highly organized and efficient, and operate like a legitimate business. They produce and distribute drugs on a massive scale, and use violence and intimidation to protect their profits.

Understanding these models is crucial for security services and law enforcement agencies. Different models of organized crime require different strategies, and incorporating them into a single model can facilitate the task of finding appropriate perceptions of the future of organized crime. For instance, the "hierarchical model" suggests focusing on leadership in complex criminal organizations, while the "patron-client model" indicates that key actors can be replaced over time, rendering them irrelevant in organized crime organizations (Rostami, 2016, p.18, 58).

Organized crime refers to illegal activities carried out by groups of individuals, who work together to achieve common goals. Organized crime can take many forms, including drug trafficking, money laundering, human trafficking, and cybercrime. To combat organized crime, law enforcement agencies use various methods, including intelligence gathering, surveillance, and investigation. In recent years, there has been a growing interest in incorporating different models of organized crime into law enforcement strategies. By studying different models of organized crime, law enforcement agencies can gain a better understanding of how criminal organizations operate and how they might evolve in the future. This understanding can help law enforcement agencies to predict the future of organized crime and develop effective strategies to combat it. One approach to incorporating different models of organized crime is to focus on the activities of both leaders and key actors in criminal organizations. In summary, incorporating different models of organized crime into law enforcement strategies can help to predict the future of organized crime and develop effective strategies to combat it. By focusing on the activities of both leaders and key actors in criminal organizations, law enforcement agencies can gain a better understanding of how these groups operate and identify vulnerabilities that can be exploited to disrupt their activities.

Law enforcement authorities are focused on understanding the intricate network of relationships within local and global organized crime syndicates. They aim to identify the link between organized crime and

corruption, and to understand its root causes, in order to design prevention programs and strategies that can control organized criminal activities. These efforts include actions such as managing personnel behavior, implementing effective query and computer systems, and providing training programs that minimize the impact of organized crime. Additionally, law enforcement agencies are committed to developing criminal statistics and research, guiding criminal justice agencies, and detecting general trends in crime. International cooperation mechanisms are also being activated to reduce the occurrence of organized crime. To better detect future trends of organized crime groups, law enforcement agencies rely on advanced analytical models to monitor criminal activities. (Asean, 2010, p. 101)

4.4: Planning for New Strategies to Combat Organized Crimes & Cyber Crimes

Current failures in law enforcement and criminal justice agencies may also be due to a reliance on accurate forecasting of future criminal activities. Rather than solely relying on predictive models, we must consider alternative approaches, such as the patron-client model, in order to more accurately describe and prevent future criminal activities. In order to effectively combat organized crime, we must learn from the lessons of the past. It's clear that relying solely on bureaucratic hierarchy to predict future criminal activities has failed us in the past. Therefore, it's imperative that we advocate for the integration of different models to better understand organized crime and prevent future criminal activities. Moreover, it is necessary to effectively combat organized crime, we must prioritize prevention over reactive measures by implementing strategies, rules, and procedures. This requires drawing upon lessons from the past and utilizing various models to gain a better understanding of organized crime, allowing us to take proactive measures to prevent future criminal activities from occurring.

strategic planners strive to equip themselves for potential organized crime activities by devising effective measures that can adapt to the evolving nature of crime, especially in countries that share borders with neighboring countries that have high crime rates and low resilience. Examples of such countries include Greece, Angola, Bolivia, and Djibouti (Shaw, 2021, p. 100-101). Since the future is uncertain, planners can only offer insights at the national, regional, and continental levels, which can inform predictive models of organized crime environments. By gaining a better understanding of emerging trends in crime, criminal justice services can accumulate intelligence over time and respond more effectively to new and evolving criminal activities.

Strategic planning is critical to enhancing the capacity of criminal justice agencies to reduce future crime and provide social protection. When done with the participation of all levels of society, it can have positive implications for sustainable development, victim protection, and the

reduction of psychological and financial damage caused by crime ((Al-Agha, 2009)). Additionally, effective planning can reduce the financial burden of criminal justice and foster a better understanding among law enforcement personnel of the factors and motives behind criminality. Ultimately, it helps protect members of society from the dangers and threats of organized crime, both domestically and abroad (Garib, 2017, p.24). However, for this to happen, decision-makers must focus comprehensively on the changing landscape of organized crime and use analytical models, rather than relying solely on quantitative analysis. They should also work to remove legal and legislative constraints that hinder their efforts to fight crime and achieve results. By adopting these strategies, criminal justice agencies can create a more effective and efficient approach to crime prevention that promotes safety and security for all members of society.

Organized criminal groups have greatly benefited from advancements in science and technology, which have made it increasingly difficult for law enforcement agencies to predict their capabilities and anticipate the full extent of their activities. As a result, computational predictions have proven ineffective and agencies must instead assess the possibilities for future criminal activity, though this process remains uncertain (Shaw Kemp, 2012, p. 27). Accordingly, It is proposed that the developing police intelligence systems and supporting legislative and legal investigation efforts to monitor individuals and entities involved in organized crime activities and to provide early detection of their risks and threats through the use of the national and global information, data and facts system.

Our findings suggest that planning is crucial for enhancing security capacity against organized crime. New trends in combating crime require a preventive approach based on scientific and technological development. Addressing organized crime now involves a more realistic strategic view, with intelligence used to channel police resources and field achievements. Strategic science provides justice agencies with an analytical focus that modifies their traditional intelligence. Relying solely on criminal laws and punitive procedures is irrelevant. Case studies may help criminal justice agencies overcome practical problems. It is essential to ascertain the significant consequences and implications of the shift from traditional to modern approaches to combating organized crime.

4.5: The Prospective Dimensions of the Future:

According to Nafeh (2017, p. 14), looking ahead involves having a comprehensive understanding of future directions and identifying potential alternatives. It requires individuals to choose the best course of action and guide their decisions towards a better future. This entails anticipating the nature and significance of future developments and being prepared to adapt accordingly. It is crucial to recognize that

today's decision-making is intrinsically linked to the security outlook of the future. As Jameel (1988, p. 90) notes, a security decision involves a series of actions, including assessment, analysis, and the identification of alternatives. The ultimate goal is to stabilize the best alternative that aligns with the decision of the authority holder. Therefore, effective decision-making today is crucial to ensuring a secure future. By proactively identifying potential risks and opportunities, individuals and organizations can take the necessary steps to mitigate risks and seize opportunities. This requires a forward-looking approach and a willingness to adapt to changing circumstances (Jameel, 1988, p. 90).

In the past, talking about the future was often dismissed as fanciful musings or mere guesswork. However, since the Second World War, administrative, security, military, and academic leaders have recognized the importance of proactively considering potential future events. They have made concerted efforts to develop strategies for preparing and responding to unforeseen challenges. Today, leaders ask themselves critical questions, such as What if something happens in the future? and how can we plan for it? They also seek to identify the most effective methodologies for addressing these challenges.

Anticipating future developments is an essential obligation for security institutions and criminal justice organs. It is no longer a luxury but a necessity to proactively prepare for upcoming changes by utilizing advanced surveillance tools. This approach is particularly crucial when it comes to tackling organized crime, which demands a readiness to confront its root causes and contributing factors to effectively prevent or minimize its impact. (Cornish and Sharif, 2016, p. 4; Loveridge, 2016, p. 125-128; Summer, 2022, p. 999-1001; Al-Senussi, 2021, pp. 56-58; Al-Hajjawi, 2021, p. 109). The future is not predetermined, but rather a malleable realm of possibility. By considering past, present, and future trends, we can create a comprehensive map of possibilities that allows us to weigh available options against preferred outcomes. This approach helps us mitigate risks and threats posed by future variables and contributes to the development of strategic planning based on future projections. By generating innovative scenarios, it can increase the efficiency and effectiveness of criminal justice agencies in their fight against organized crime (Nafeh, 2017, p. 5, 6).

In the field of security, anticipating future changes and implementing strong and adaptable strategies are crucial for developing effective measures to combat a range of criminal activities. Criminal justice agencies face significant challenges in staying ahead of evolving crime trends, making the ability to forecast and plan for future criminal behavior essential for success. To mitigate risk, there must be a focus on utilizing effective tools and techniques for strategic planning. This involves identifying potential threats and developing proactive measures to address them. By staying ahead of criminal activity, security professionals can reduce the likelihood of threats and improve overall

safety (Ballard, 2016). In summary, a forward-thinking approach that emphasizes robust and flexible strategies, along with effective strategic planning, is necessary to combat crime effectively in today's rapidly changing security landscape. Scenario analysis is a valuable strategic planning method that can be used by criminal justice agencies to develop adaptable and sustainable strategies for tackling organized crime. To do this, analysts must create realistic scenarios that provide decision-makers with creative and plausible depictions of a desirable future world. While these scenarios should be logical and grounded in reality, they should also consider the possibility of significant challenges, problems, and obstacles that may arise unexpectedly. As such, analysts may need to explore potential scenarios that are uncomfortable or even uncomfortable, but still possible (Ballard, 2016).

In brief, predicting future organized crime is an investigative strategy that aims to identify potential criminal activities before they occur and take preventive action. Analysts employ predicting future organized crime by gathering and analyzing information on current criminal phenomena from internal and external sources to identify criminal activities, times, locations, and persons involved. Decision makers can use this information to channel security resources and reduce organized crime and its security threats. However, strict measures are necessary to protect individuals' rights and privacy, as well as respect suspects' constitutional rights when using this strategy.

Based on the preceding discussion, we propose that the future of organized crime can be analyzed by using two approaches. First, the exploratory extrapolation approach, which requires decision makers to begin with the present and use past data to project possible or predictable scenarios for the future. Second, decision makers can adopt a normative and targeted approach by starting with desirable future goals and positions and working backward to determine appropriate pathways from the present to the future (Zahir, 2004, p. 53). Regardless of the approach taken, decision makers must conduct an "information and potential" analysis of the future criminal phenomenon. This analysis should include an examination of the "political, social, economic, and technological" environmental factors, as well as an assessment of the strengths and weaknesses of the variables that contribute to the criminal phenomenon. Law enforcement data must also be analyzed to ensure a comprehensive understanding of the issue at hand. Only through a thorough examination of these factors can decision makers formulate informed and effective strategies for addressing organized crime in the future.

Finally, it can be concluded that the decision makers may consider various hypotheses regarding organized crime, such as its dependence on social, economic, and political conditions; its threat to national security and resulting damages; its focus on profitability; its need for careful organization and planning; its use of sophisticated

communication and concealment techniques; its susceptibility to technological and social changes. To prepare for future organized crime, decision makers should collect and analyze data on current crimes, use prediction methods to identify criminal activities and perpetrators, analyze data using statistics, AI, and math, draw conclusions on the causes of organized crime, and develop strategies for prevention and improved security operations through cooperation and governance.

4.6: Contemporary Security Techniques:

Security surveillance techniques use artificial intelligence and data analysis to significantly identify potential risks and future crimes. Some of the main means of contemporary security surveillance are as follows:

Big Data Analysis: Large amounts of data are collected from various sources, such as social media, communications records, photos, videos and texts. This data is analyzed using machine learning and artificial intelligence techniques to identify possible patterns, trends and risks (Mohammed, 2022, p. 101). Big data analysis is the process of collecting and analyzing large and complex data to detect criminal activities by using modern technologies in the field of data science and artificial intelligence (Ali, 2018, p. 422). These techniques include the use of statistical modelling, machine learning, geographic and network analysis of data and other modern methods (Babylon, 2019, p. 76). Big data is collected from multiple sources such as social networks, forums, e-mails, conversations and other online data sources as well as from other data sources such as banks, information centers and legal enforcement agencies. After data collection, it is analyzed using artificial intelligence and data science techniques. Statistical modeling techniques are used to analyze data and predict possible patterns of criminal activity. Geographic analysis is used to monitor areas with the highest crime rates, and web analysis is used to monitor relationships between criminals and criminal activities. One example of the successful use of big data analysis to detect criminal activity is its use in the fight against drug trafficking and terrorism. Thanks to the use of artificial intelligence and data science techniques, competent authorities in various countries of the world have been able to monitor, investigate and arrest criminal activities (Babylon, 2019, pp. 82-87).

Big data analysis can help detect potential organized crime by analyzing patterns and relationships in large data and debriefing hidden and crime-related information. Big data analysis can also help identify suspicious and habitual activities of suspects, identify their behavioral patterns, and locate their places, time and social networks (Genphussi, 2012, p. 95). Since organizations' crimes usually involve mutual cooperation among many individuals, analysis of big data can help to uncover links and relationships between suspects and other related activities. For example, big data analysis can help detect suspicious financial transactions in suspects' bank and financial accounts. Analysis

of big data can also be used to detect foreseeable criminal activities in designated areas and at specified times, such as theft, fraud, drug trafficking and others.

Background checks: Traffic records and persons' information, such as crime records, criminal evidence, medical and financial history, are analyzed. This information is used to identify potential suspects and assess potential risks, and backchecking (or past verification) is one of the important tools contributing to the detection of future organized crime (Zine El Abidine, 2013, p. 292). This method involves using historical data and available information to analyze patterns and trends and identify relationships between events, individuals and those involved. Examples of how back-checking can be used to detect future organized crime: back-checking may be used to analyze past activities of organized groups to determine the patterns of behavior and tactics they use, and this information can be used to identify weaknesses in the judicial system and improve future action against crime. Background verification can also be used to analyze previous communications data and financial transactions of suspicious individuals and organizations (Khalil, 2018, p. 28). This helps identify links between individuals and organized groups and find out how to fund their activities. Rear verification may be used to analyze location guides, traffic verification and public transport system. This information can be used to identify possible models of movements of organized groups and areas of activity, or to analyze past events and geographical details to identify places used to organize offending activities and to determine the pattern of activity in these areas (Caliph and Saeed, 2015, pp. 198-199).

Behavioral Analysis: Behavioral analysis techniques are used to identify unusual behaviors and changes in people's or institutions' behavioral patterns. This data is analyzed to identify potential risks and future crimes (Farouk, 2012). Behavioral analysis can also be used to detect potential organized crime by examining the behaviors of suspected individuals and organizations. For example, the organization's activities can be examined and thus compared with the known patterns of activity of organized crime groups (Al Mutawa, 2018, p. 45). Records of communication and communications between the organization's personnel, which may show suspicious or covert communication, could also be studied, indicating the potential for organized crime activity. Financial and funding records can also be studied and sources verified (Hussain, 2012, 657). Organized crime usually depends on illicit funds, and behavioral analysis can be used to determine whether the organization's financial transactions are in line with known funding patterns for organized crime groups. For example, behavioral analysis can be used to analyze the unusual activities of specific individuals in the organization, such as increasing financial deposits in their accounts, or increasing the number of business transactions they conduct. The pattern of individuals' daily activity can also be studied and compared to common models of organized crime activities. In general, behavioral

analysis can be used to identify unusual or suspicious activities that are compatible with organized crime patterns, which can indicate the existence of organized crime. This is done by analysing and controlling general behaviors and regular models.

Geographic Analysis: Digital mapping and GIS techniques are used to identify areas with high crime rates (Faqir and Alrousan, 2023, p.107). This data is analyzed to identify potential risks and allocate resources effectively (Arasan, 2022). Geographical analysis can be used to detect future organized crime by analyzing geographical data on suspicious crimes and activities in different regions. This typically involves the collection of geographical data on suspicious crimes and activities from different sources, such as police records, media reports and local community information. The data are analyzed using geographical data analysis tools, which allow the analysis of geographical data in different ways, such as temporal analysis, geographical density analysis and analysis of geographical relationships between crimes (El Dub, 2021, p. 237-238). The results of the analysis can also be used to identify areas at risk from organized crime, focus security efforts on these areas, and use geographical analysis to develop effective strategies for the prevention of organized crime, and intervene quickly when such crimes occur (Nassa, 2018, p. 243), as well as strengthen cooperation and coordination between various government agencies and the community in the fight against organized crime.

Intelligence Work: Intelligence work is used to detect potential organized crime by collecting, analyzing and interpreting information to generate useful information that helps detect crimes and criminals (Al-Sharif, 2021, 344). This is done through the application of a range of intelligence techniques, methods and tools which include (Aidan, 2007, p. 18): First, data and information analysis: the process of analyzing data and information from multiple sources, such as documents, databases and audio and video recordings, transforming them into useful and usable information, and second, verification and investigation: It is the process of verifying the authenticity of available information, verifying the authenticity of forensic evidence, obtaining additional information to help detect crimes and, thirdly, cooperating and coordinating: It is to cooperate with relevant stakeholders in the Government, the police, international organizations and other relevant bodies to exchange information and enhance capabilities and efforts to detect organized crime (Burcher and Whelan, 2018, Pp. 2-4).

Examples of effective use of intelligence work in detecting potential organized crime include tracking the drug trade: intelligence work is used to gather and analyze information about drug trafficking networks to determine the pattern of drug traffic and the fraud methods used by the networks, and financial crime detection: intelligence work is used to gather information about money transfers, verification and analysis.

4.7: Contemporary Trends in the Prevention of Potential Organized Crime:

Contemporary trends in the prevention of potential organized crime indicate the adoption of multilevel strategies, including law, regulation, international cooperation, technology and community awareness. Among these trends are:

Haresh laws and legislation: This includes eliminating gaps in existing laws and developing them to include new organized crimes. This also includes increased and tighter penalties to prevent offenders from committing further crimes (Brizat, 2004, 166-167). Tightening laws and legislation is part of the solutions available to combat organized crime, and it is important that Governments take strong legal action to reduce organized crime activity (Rizwan, 2019, p. 27-28), for example, enacting laws and legislation that deal strictly with crimes related to organized crime, such as drug trafficking, human trafficking and money-laundering, and improving the judicial system's capacity to combat organized crime, by training judges and prosecutors in dealing with organized crime, and providing the necessary resources to do so. It also strengthens government control over business activities suspected of dealing with organized crime by monitoring bank accounts and verifying financial sources, improving security measures in areas where organized criminals are active, and enhancing cooperation between local and national security actors.

Legislative gaps that allow organized crimes to occur vary from country to country and from law to law. However, some common gaps that might prevent the implementation of regulated laws could be identified. One of these gaps is the weakness of the judicial system, which can result in the law not being properly imposed on organized offenders, and a failure in the laws governing organized offences, which can leave room for offenders to work. Also, corruption contributes to undermining the implementation of laws, where bribes and influences can be used to avoid accountability in addition to geographical boundaries where organized criminal border activities pose a challenge to governments and cause difficulty in determining responsibilities, sometimes organized crimes are ignored because of legal separation. s rights ", which meant that some practices that might be illegal in certain countries could be legal in others.

International cooperation: This includes the exchange of information and experience between Governments and international institutions and cooperation in criminal proceedings, prosecution and extradition. Combating organized crime is an international challenge that requires strong cooperation between states to address this phenomenon (Mohammed, 2019, p. 8). One of the most important proposals and solutions for the development of international cooperation in this area is the strengthening of international cooperation and coordination among

States through the exchange of information, experiences and successful experiences, the identification of effective strategies to counter them, and the improvement of international legislation and laws on combating organized crime (Mohammed, 2019, pp. 652-653), ensuring their effective application, and strengthening cooperation between judicial authorities in different States, through the exchange of information, experience and judicial techniques through the provision of training, modern technology, the exchange of experiences, the establishment of strong security partnerships and the strengthening of regional cooperation (Mohammed, 2019, pp. 10.11) and promoting public awareness about the seriousness and impact of organized crime on societies, stimulating active participation in combating it, as well as working to eliminate factors that facilitate the spread of organized crime, by working to improve the economic and social situation in States and combat poverty.

Modern technologies: This includes the use of advanced technology such as artificial intelligence, facial recognition and cloud computing to analyze data and identify organized crime activities. Modern technology for the prevention of organized crime can be used in a number of ways. First, massive data analysis (Al-Shamsi, 2022, p. 101-103): large data analysis techniques can be used to analyze data on organized crime and identify suspicious patterns and behavior. This data can be used to guide investigative and intelligence efforts, and the second is artificial intelligence: Machine learning and artificial intelligence can be used to detect suspicious behavior and analyze images and videos to identify suspicious people, places and objects, third encryption and cyber protection: encryption and cyber protection technologies can be used to protect and secure sensitive data and information against hack, theft and manipulation, and fourth smartphone applications: Smartphone apps can be used to report suspicious crimes, contact the police and assist in the investigation.

Modern technology is used in many countries to prevent organized crime. In the United Kingdom, big data analysis technology has been used to reduce organized crime and control the cross-border movement of illicit drugs and weapons. Modern technology has also been used in China to monitor social activities and verify the identities of suspicious persons (Babylon, 2019, p. 121). In the United States of America, artificial intelligence techniques have been used to prevent organized crime through the use of data analysis and machine learning techniques to analyze potential criminals' data. Predicting areas that could see a rise in crime rates and identifying images to identify suspects and potential offenders by analyzing images captured by street-mounted cameras, Graphic analysis of communications, mobility and financial transactions records of suspects and potential suspects and the detection of illicit weapons at airports, ports and border ports to prevent the transfer of weapons, explosives and dangerous materials, Use of the industrial intelligence approach to analyze data and information on organized

crime and criminal networks and identify suspicious activities and potential threats.

Training and development: It includes the provision of training, education and continuous improvement of legal and security workers' skills to enhance their capacities in combating organized crime. Training and development is an effective tool in the fight against organized crime, providing policemen and investigators with the knowledge and skills needed to deal with this type of serious and sophisticated crime. An example of effective training and development in the fight against organized crime is police training in the use of advanced technology in evidence collection and forensic analysis assistance to better identify and track offenders and train them in effective cooperation and coordination with local and international stakeholders to provide them with the information necessary to analyze and interpret the activities and movements of offenders, as well as their training in the use of modern methods to verify individuals' identity and verify official documents to prevent the use of false identities and better identify perpetrators, Analysis of available forensics and identification of relationships between crimes, which helps to interpret and identify criminal patterns and detect organized groups, In addition to their training in the use of effective interrogation and verification of information and testimony criminal activities ", helping to obtain the information needed to analyze criminal activities and detect offenders.

5. CONCLUSION

Security agencies can use surveillance technologies to detect and prevent organized crimes. This involves using available data and information, including geographical, social, economic, behavioral, and criminal data, and then analyzing this data using artificial intelligence, machine learning, and predictive analytics to identify common patterns and models in organized crimes, as well as predict locations, times, and individuals at risk. Surveillance technologies for organized crimes are used in many areas such as combating drug trafficking, human trafficking, smuggling, financial crimes, fraud, forgery, and terrorism. Security agencies also use surveillance technologies to analyze criminal information, verify the validity of criminal data and evidence, and enhance international cooperation in the fight against organized crimes. It is worth noting that the use of surveillance technologies must be carried out in a legal and ethical manner, with respect for individual rights and privacy. It must be within a specific legal framework and with the approval of the relevant authorities.

The current study provides a number of recommendations that should be followed when using security surveillance technologies to combat organized crime, which are as follows:

1- Ensure the suitability of using security surveillance and criminal analysis technologies for specific criminal control purposes, and ensure that they are only used within a legal and ethical framework.

2- Ensure the availability of sufficient resources for security agencies to implement effective strategies to combat organized crime and use security surveillance technologies efficiently.

3- Provide appropriate training for employees responsible for data analysis, security surveillance technologies, and machine learning to obtain accurate and useful results.

4- Adhere to privacy and security standards when collecting and analyzing personal data and maintain the confidentiality of this data.

5- Work in an integrated manner with other relevant entities, such as government and private institutions and civil society, to enhance cooperation, exchange information, and share experiences in the field of combating organized crime.

6- Continuously evaluate the effectiveness of security surveillance technologies, data analysis, and constantly update and improve them to meet the changing challenges in combating organized crime.

Bibliography

Ahmad Dhuqan Al-Hindawi, Saleh Salim Al-Hamouri and Rola Nayef Al-Mu'ayyah Al-Mu 'aqiyah, The Vision of the Future and Smart Readiness, National Media Council, United Arab Emirates, 2017.

Ahmad, Muhammad, Ahmad Ayasra, and Farah Zawaideh. "Issues and problems related to data quality in AIS implementation." International Journal of Latest Research in Science and Technology 2.2 (2013): 17-20.

A. Y. A. B. Ahmad, S. S. Kumari, M. S, S. K. Guha, A. Gehlot and B. Pant, "Blockchain Implementation in Financial Sector and Cyber Security System," 2023 International Conference on Artificial Intelligence and Smart Communication (AISC), Greater Noida, India, 2023, pp. 586-590, https://doi.org/10.1109/AISC56616.2023.10085045.

Ahmad Yahya Bani Ahmad, Nawwaf Hamid Alfawaerah, Anas Al-Qudah, Mahmoud laham. The Governance Capability to Support Accounting & Financial Disclosure in the financial Statements (Case Study – Industrial Sector) , Research Journal of Finance and Accounting www.iiste.org ISSN 2222-1697 (Paper) ISSN 2222-2847 (Online) Vol.4, No.10, 2013.

Ahmad, A. Y. Bani ahmad , (2019). Empirical Analysis on Accounting Information System Usage in Banking Sector in Jordan. Academy of Accounting and Financial Studies Journal, 23(5), 1-9.

Aidan Wells, Understanding Intelligence Supervision, Guide, Translation of Mahmoud Sayed, Geneva Centre for Democratic Control of the Armed Forces, 2007, p. 18. 1-108. On the website: https://www.dcaf.ch/sites/default/files/publications/documents/Intelligence_Oversight.pdf

Al-Agha, Ismail Wasefi Ganem, The Misuse of Internet and Mobile Technology and Their Role in Deviating Events in the Gulf Cooperation Council Countries, PhD Thesis, Naif Arab University for Security Sciences, 2009.

Ali Alsheikh GA, Binti Abd Halim MS, Ayassrah AYA, Theeb Alnawafleh EA, Bin A Tambi AMS. (2018) Investigation of Factors Influencing Customer Loyalty in Malaysia and Jordan Hotel Industry. J Hotel Bus Manage 7: 181. doi: 10.4172/2169-0286.1000181

Al-Dob, Tariq Abdulaziz, Using Time Chain Analysis Models to Predict the Total Crimes in Kuwait, Journal of Gulf and Arabian Island Studies, 47 (181), 2021, 235-248.

Ali, Ahmed Khairy Abdallah, Big Data and Analysis: Concept, Characteristics and Applications, Faculty of Arts Journal, 49 (2), 2018, 411 - 444.

Al-Kilani, Ismail Gharib, History and Future Industry, Nation Journal, vol. 6, No. (69), 1986.

Al-Shamsi, Juma Sultan Saif, Modern Technologies and Smart Programs and Its Role in the Fight against Crime and Drugs, Journal of Legal and Economic Research, 55, 2022, 87-146.

Al-Sharif, Mahmoud Salama Abdulmunim, Legal Nature of AI Crime Prediction and Legitimacy, Arab Journal of Forensic and Forensic Sciences, 3 (2), 2021, 341-359.

Amir Rostami, Criminal Organizing: Studies in the Sociology of Organized Crime, Stockholm University, 2016, Pp 18, 58. https://www.diva-portal.org/smash/get/diva2:921818/FULLTEXT01.pdf (accessed on 16 March, 2023)

Amr Ezzat Al-Ho, Supervision of Security Work between Theory and Practice, Journal of Legal and Economic Studies, vol. 9, No. 1, 2023.

Arendt, Hannah, Between Past and Future: Six Exercises Political Thought, New York, the Viking Press, the Macmillan Company of Canada Limited, 1961. 1-256.

Arsan, Abdullatif, Geography and its Place on the Security Map, Security and Life Journal, 21 (239), 2002, 42-55.

Babylon, Amar Yasser Mohamed Zuhair, The Role of AI Systems in Predicting Crime, Policing Thought, 28 (110), 2019, 59 - 133.

Ballard, Dagon Randall, Strategic Planning, National Shield Magazine, Directorate of Moral Guidance in the General Command of the Armed Forces, United Arab Emirates, 2016.

Brantingham, P.J., Brantingham, P.L., & Andresen, M.A. (2017). The geometry of crime and crime pattern theory. In

Bani ahmad , Ahmad A. Y.(2013).The Ability of Accounting Information Systems to support Profitability and Growth (Industrial Sector-Jordan Companies)European Journal of Business and Management www.iiste.org ISSN 2222-1905 (Paper) ISSN 2222-2839 (Online) Vol.5, No.19, 2013.

Burcher, M. and Whelan. C., Intelligence-Led Policing in Practice: Reflections from Intelligence Analysts, Police Quarterly, 2018, 1-21.

Burizat, Jihad Mohammed, Majali, Tawfiq Regime, Organized Crime: Analytical Study, Master's Thesis, University of Mutah, Karak, 2004, 1-190.

Dhanayeb Aasi, International Mechanisms against Transnational Organized Crime, Master's thesis, Faculty of Law and Political Science, University of the Munteri Brothers, Constantine, Algeria, 2010.

Donis Loveridge, Staging: Art and Proactiveness of Science and Art The: Foresight, Editorial Board Translation, Future Studies Review, No. 1, 2016, p. 125, 128.

Edward Cornish and Hassan Al-Sharif: Future Exploration Curriculum, Future Studies Review, Issue (1), 2016.

Faqir, Raed S A, Alrousan, Ehab, Chaos Theory and the Geography of Crime, Chapter in Book, edited by Pramod Kumar Singh, Perspective in Laws, AkiNik Publications, New Delhi, Volume (6), 2023, 101-129.

Farouk Jamil, Impediments to Administrative Development in Lebanon, T1, Dar El Gail, Beirut, 1988.

Farouk, Shirin, Behavioral Analysis Reveals the Nationalities of Criminals, UAE newspaper Al Bayan, April 4, 2012, online: https://www.albayan.ae/across-the-uae/accidents/2012-04-04-1.1624184

Garib, Hakim, Risks of Social Media on Community Security: Stakes and Strategies, the international Scientific Seminar on "Globalization of political media and challenges to national security of developing countries," Tuesday, April 11, 2017.1-28.

Genphosi, Abdulaziz, Mechanisms Developed by INTERPOL to Address Organized International Crime, Journal of Police Thought, 21 (83), 2012, 75 - 110.

Hussain, K. Zakir, M. Durairaj, and G. Rabia Lahani Farzana, "Criminal Behavior Analysis by Using Data Mining Techniques," presented at the IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM -2012), March 30-31, 2012. 656- 658.

Ihab Fouad Mustafa Al-Hajjawi, UAE Security Policy Outlook for Future Regional Challenges, Journal of the Faculty of Commerce for Scientific Research, Issue (72), 2021

Khalifa, Badr Khalid, and Said Abdul Latif Ismail, Protection of National Security, Information and Communication Security and the Internet against Terrorism, Organized Crime, Penetration, Espionage and Surveillance: From a Strategic Rights and Security Perspective, Kuwait International Law College Journal, 3 (10), 2015, 163 - 280.

Khalil, Alaa Mohammed Abdullah, Ashraf Osman Ibrahim, Discover Distorted Fingerprints Using Neural Networks, Master's Thesis, Nilin University, Khartoum, 2018, 1-70.

Khan, Yasser, et al. "Application of Internet of Things (IoT) in Sustainable Supply Chain Management." Sustainability 15.1 (2022): 694. https://doi.org/10.3390/su15010694

Klaus von Lampe, The Use of Models in the Study of Organized Crime, Paper presented at the 2003 conference of the European Consortium for Political Research (ECPR), Marburg, Germany, 19 September 2003.

l Mutawa, Noora Ahmad, Integrating Behavioral Analysis within the Digital Forensics Investigation Process, PH.D Thesis, Doctor of Philosophy, University of Central Lancashire, 2018. 1-236.

Maouqbel, Ziad, Black Actor in Global Politics: A Reassessment of the Place of Transnational Organized Crime in Contemporary Global Politics, Journal of the Arab Future, vol. (41), No. (477), 2018.

Marc Choo, World Organized Crime Indicators, Global Initiative against Transnational Organized Crime, 2021

Mark Shaw and Walter Kemp, Vandals' Watch: A Guide to the Analysis of Organized Crime in Fragile States, International Peace Institute, New York, 2012.

Mohammed, Al-Hassan Sha'aban Ahmed, Big Data, Its Essenes, Significance and Elements, Arab International Journal of Knowledge Management, 1 (2), 2022, 99-148.

Mohammed, Sara, International Cooperation in Extradition in Light of National Legislation and International Conventions, Journal of Sharjah University of Legal Sciences, 17 (1), 2019. 646-677.

Mohammed, Suleiman Abdulwahid Abdallah Ahmed, Security Cooperation to Counter Organized Crime, Journal of Legal and Economic Research, 49, 2019, 1 - 45.

Najmuddin, Samer Samir, Cyber Organized Crime: Analytical Study in Palestinian Legislation, Journal of the Islamic University for Shari 'a and Legal Studies, vol. 29, No. 2, 2021.

Nasissa, Fatima al-Zahra, and Fatima Zuaiter, Organized Crime Under Current Changes, Journal of Historical and Social Studies, 34, 2018, 237-245.

Rizwan, Reza Abdul Hakim Ismail, INTERPOL between International Law and UAE Legislation: A Comparative Analysis of the Application to the UAE police system, Journal of Security and Law, 27 (1), 2019, 13-64.

Said Abdu Nafa, Strategic Supervision for the Future, Arab Journal of Educational and Social Studies, Issue (11), 2017.

Snoussi Mohammed al-Senussi, looking ahead is essential to understanding our self and reality, Islamic Consciousness Magazine, vol. 59, No. 679, 2021.

Summer Consultation, Looking Ahead: Methods for Predicting the Future in International Interactions Model Scenario, Journal of Legal and Political Research, vol. 7, No. 1, 2022.

Wortley R. & Townsley M., Environmental Criminology and Crime Analysis, 2nd ed., New York, NY: Routledge, 2017, Pp. 98 – 115.

Zayn El Abidine, Jaafar, and Bassam Hassan Kabir Al-Melhani, Fixed Facial Recognition Using Neural Network Rear Diffusion Algorithm, Postgraduate Journal, 2, 2013, 279-294.

Zia al-Din Zahir, Introduction to Future Studies, Concepts, Methods, Applications, Arab Center for Education and Development, Book Publishing Center, Cairo, 2004