Decrypting the Balkan underworld. A theoretical analysis of encrypted communication in organized crime

Assoc. Prof. Dr. Fabian ZHILLA
(ORCID ID: https://orcid.org/0000-0001-5929-9674)
Department of Business & IT Canadian Institute of Technology (CIT), Tirana, Albania
fabian.zhilla@cit.edu.al

Abstract

This article delves into the pervasive deployment of encrypted communication platforms within Balkan criminal entities, including Albanian organized crime, offering a meticulous examination and legal scrutiny spanning the period from 2019 to 2023. Focusing primarily on communication channels such as "Matrix," "Sky ECC," and "EncroChat," this study unveils the intricate interplay between these technologies and criminal activities, shedding light on their implications for investigation of such sophisticated organized crime groups. Case studies of Balkan Mafia on the use of EncroChat and Sky ECC during 2019-2022 reveal their unprecedented influence on criminal activities, offering anonymity, non-traceability, and facilitating organized crime on a global scale. This research employs a multifaceted methodology that seamlessly integrates descriptive analysis, literature review, and theoretical exploration. It supports an inclusive perspective, urging scholars and policymakers to move beyond outdated frameworks to effectively combat the evolving impact of organized cybercrime on societies worldwide.

Keywords: *cybercrime, Sky ECC, EnroChat, Balkan mafia, Albanian organized crime, hybrid communication, technological shift*

Introduction

The relentless progress of technology has instigated profound changes in societal structures, concurrently driving a transformation in criminal methodologies. Within the contemporary digital landscape, the activities of organized crime groups have undergone discernible influences. This digital terrain accommodates a diverse array of organized crime entities, each characterized by distinct organizational models. This spectrum encompasses the sophistication of communication methods employed by organized crime groups, leveraging advanced technological means. Hybrid communication forms are evolving, characterized by the integration of human-machine collaboration within networks that encompass both human and non-human participants.

A pivotal dimension of this evolution lies in the utilization of encrypted communication platforms, notably exemplified by EncroChat and Sky ECC. These technologies have precipitated a paradigm shift, enabling a spectrum of organized crime activities that range from technologically sophisticated endeavors to more conventional practices. The smooth shift between online and offline realms is enabled by the strategic utilization of encrypted communication tools. Criminal organizations, operating at both local and transnational levels, have traditionally utilized encrypted messaging systems to evade surveillance. Companies like Sky Global offered comprehensive services, including phone modifications to disable cameras, microphones, and GPS, automatic deletion of messages after a designated period, and resistance to cooperation with authorities (Saito, 2021).

The successive shutdowns of EncroChat and Sky ECC have sparked optimism that this technological advantage will be temporarily diminished. The closures have dealt a significant blow, particularly in Belgium and parts of the criminal market in the Netherlands, where Sky ECC was highly trusted as a secure communication system. According to police experts the police now possess extensive information on the underworld's structure, bank accounts, and corrupt contacts, leading to the arrest of numerous individuals. The unraveling of these networks, which took years to establish, signifies a major setback for criminal organizations (Saito, 2021). The use of these platforms, however, should be seen with the lenses of a shift of the organized crime groups to a different age and model, the so called digital "criminal" area.

Theoretical discussion

The confluence of technology with criminal enterprises has eroded the heretofore unequivocal delineation between the corporeal and virtual dimensions inherent to organized criminal activities. Despite these profound shifts, it is evident that existing criminological theoretical frameworks have yet to fully absorb the transformative ramifications of the digital society, particularly regarding the deployment of encrypted communication tools like EncroChat and Sky ECC by organized crime entities. This gap underscores the imperative for the formulation of contemporary research hypotheses within this context (Di Nicola, 2022).

While there is a scholarly exposition which delves into the inquiry of conventional distinctions between offline/online or physical/digital crimes, what is missing is the classification of certain advanced technological features of organized crime groups, particularly those leveraging encrypted communication platforms like SKY ECC and EncroChat, as organized crime entities. This categorization may hinge into the adoption of a contemporary and adaptive framework for understanding the new perspective of the sophistication of organized crime. Several studies have drawn the attention to the use of technology by organized crime as an indicator of quick adaptation to the new digital sociology of the criminal world.

Referring to the literature review of main theoretical threads by Whelan, Bright and Martin (2023), one may argue that encrypted methods of communication by organized crime groups should not come as a surprise. We live in i digital criminal area, what Powell et al., (2018) calls it a "digital criminology" contending that conceptualizing technological and non-technological aspects as two different or yet oppositional categories are no longer valid to an over digitalization of societal mindset. Other authors support this paradigm by emphasizing that technology is now a contemporary tool for breaking cyber security (Dupont & Whelan, 2021), committing crimes online (Mackenzie, 2022), enabling violence on online platforms (Henry et al., 2020) and facilitating the communication of organized crime (Di Nicola, 2022).

Di Nicola (2022) introduces the concept of "digital organized crime," offering an interpretive framework to capture how encrypted communication platforms, notably SKY ECC and EncroChat, may induce shifts in the organizational structures of criminals and their activities. The unfolding of organized crimes within a digital society follows a continuum, determined by the extent to which criminal groups, particularly those employing SKY ECC and EncroChat, leverage these technologies. While the continuum concept is valuable, this approach, akin to other scholarly endeavors emphasizing the relevance of organized crime

conceptualizations to cybercrime (e.g., Broadhurst et al., 2014) does not explicitly address contentious elements in organized crime definitions, such as extra-legal governance as a core feature. On the other hand, Wall (2021), considers the use of technology not only for communication but also for extortion and threats.

Aligned with the perspective that narrow, inflexible definitional paradigms employing "partially obsolete frameworks" (Di Nicola, 2022) have surpassed their pragmatic utility, our contribution to scholarly discourse introduces an approach to organized crime pertinent to both traditional and cyber contexts. In this advanced academic exploration, the focus centers on the intricate dynamics of encrypted communication platforms, specifically SKY ECC and EncroChat, as emblematic exemplars in the evolving landscape of organized cybercrime. We contend that pivotal concepts integral to existing understandings of extra-legal governance, such as violence and territory, require nuanced reconceptualization to account for their multifaceted physical and digital properties, particularly within the context of these encrypted communication tools.

Methodology

This study seeks to conduct a thorough examination of the dynamic evolution of the Balkan organized crime in the digital era, concentrating on the nuanced impact of advanced communication technologies, particularly the utilization of encrypted platforms such as EncroChat and Sky ECC. The research aspires to elucidate the transformative influence of these technologies on the organizational structures and operational modalities of criminal entities. Furthermore, it aims to scrutinize the ramifications of recent law enforcement interventions, notably the closures of EncroChat and Sky ECC, on the technological prowess formerly enjoyed by criminal organizations with focus on Albanian organized crime. The overarching objective is to contribute significantly to academic discourse by providing insights into the intricate dimensions of organized crime within the context of technological advancements.

This research employs a multifaceted methodology that seamlessly integrates descriptive analysis, literature review, and theoretical exploration. The initial phase delves into a discerning descriptive analysis, shedding light on the evolving landscape of organized crime in the digital era, with a particular emphasis on the crucial role played by sophisticated communication methods. The literature review extensively draws from the works of renowned scholars, including Whelan, Bright, Martin, Powell, Dupont, Mackenzie, Henry, and Di Nicola. This compilation culminates in the establishment of a robust theoretical framework, aimed at comprehending the intricate intersection of technology and organized crime.

The theoretical discussion serves as a pivotal point for advancing the scholarly argument, proposing a nuanced reconceptualization of core organized crime constructs that takes into account the pervasive digitalization of criminal activities. Building upon the foundational work of Di Nicola in "digital organized crime," this research introduces an innovative approach relevant to both traditional and cyber contexts. It highlights the complex dynamics inherent in encrypted communication platforms. The focus then shifts to contextualizing the theoretical discussion within the sophisticated communication patterns of the Balkan mafia, with a specific emphasis on Albanian organized crime. Although the methodology does not explicitly detail empirical research or data collection, it depends on amalgamating existing scholarship and perspectives offered by various experts, often in the form of concise legal or policy analyses. This comprehensive approach aims to provide a refined understanding of the intricate interplay between technology and Balkan organized crime. Additionally, it sheds light on the profound implications of recent developments in encrypted communication platforms for the realm of criminality. The discussion on the Albanian organized crime within the Balkan mafia adds a layer of complexity and specificity to the theoretical framework, contributing to a more comprehensive analysis of the subject matter.

Findings

The findings underscore a significant gap in existing criminological frameworks, highlighting the urgency for contemporary research hypotheses. The proposed approach transcends traditional and cyber contexts, emphasizing encrypted platforms as pivotal in the landscape of organized cybercrime. This perspective challenges conventional definitions, urging nuanced reconceptualization of fundamental concepts such as extra-legal governance, violence, and territory. Case studies of Balkan Mafia on the use of EncroChat and Sky ECC during 2019-2022 reveal their unprecedented influence on criminal activities, offering anonymity, non-traceability, and facilitating organized crime on a global scale. The dismantling of these platforms by law enforcement illustrates a dynamic interplay between technology and crime prevention. Beyond EncroChat and Sky ECC, the study examines instances like Ennetcom, Phantom Secure, and platforms created by law enforcement agencies like ANOM. These examples illuminate the dual role of technology in enabling and countering organized crime, emphasizing adaptability and global reach. The integral role of encrypted communication platforms is evident in the operational strategies of Albanian criminal groups, showcasing adaptability in exploiting advanced communication technologies for illicit activities. The study supports an inclusive perspective, urging scholars and

policymakers to move beyond outdated frameworks to effectively combat the evolving impact of organized cybercrime on societies worldwide.

Originality/value

This study advocates contemporary research hypotheses that can comprehensively capture the transformative implications of these communication platforms to transnational organized crime. A distinctive focus on Balkan Mafia groups provides a nuanced understanding of the integral role played by encrypted communication platforms in their strategies. This specific lens offers insightful perspectives on how criminal entities leverage advanced communication technologies for illicit activities. In conclusion, the research emphasizes the enduring relevance and originality of the research in the dynamic field of criminology, particularly in shedding light on the multifaceted relationships between technology and organized crime.

EncroChat and Sky ECC: unveiling cybercrime dynamics (2019-2022)

The EncroChat and Sky ECC platforms emerged as prominently utilized tools by organized crime and high-ranking corrupt officials during the years 2019-2022, and this was not without reason. EncroChat phones represented a modified version of Android devices, with certain models utilizing the "BQ Aquaris X2" versions, a phone produced in 2018 by a Spanish company (Cox, 2020a). The development of EncroChat phones occurred around the period of 2015-2016, following access to the server of the Canadian company Blackberry by Canadian and Dutch authorities (Hamilton, 2020). Initially used by individuals in the business world to conceal their private lives, these phones gradually gained favor within the criminal sphere due to the services they offered (Hughes, 2019).

According to Europol, EncroChat phones facilitate encrypted communication, ensuring users complete anonymity, non-traceability of the device and client account, and swift deletion of communications from phones. These devices featured an encrypted and inconspicuous interface, devoid of traceable services or accessories such as cameras, microphones, GPS, and USB ports. They also boasted functions to secure user immunity, including automatic message deletion, a PIN code to instantly erase all data on the device, and wiping all data in case of repeated entry of an incorrect password.

These functions allowed the elimination of messages in case of device loss, use by third parties, attempted hacking, or seizure/confiscation by law enforcement

agencies. Additionally, the devices offered the capability to remotely hide messages from the service provider (seller) or through assistance provided by the seller to users online. EncroChat phones cost approximately 1000 euros, with an international usage subscription fee of 3000 euros per year, along with 24-hour customer service throughout seven days a week (Europol & Eurojust, 2020).

These phones could facilitate communication only if they had internet access, and only those in possession of them could communicate through them with a password of at least 15 characters (Hughes, 2019). The identity of the company that developed EncroChat phones is unclear, as its representatives presented the company as a legitimate business with clients in at least 140 countries worldwide. It is believed that the financiers and developers of this company are Dutch citizens, but its servers were in France, in the city of Roubaix (Sky News, 2020). As per Court Decision of the German Federal High Court, no.5 StR 457/21, date 02.03.2022, during the investigation, French authorities found nearly 66,134 SIM cards of a Dutch company.

EncroChat purportedly established sales outlets in prominent cities such as Amsterdam, Rotterdam, Madrid, and Dubai (Cox, 2020a). Nevertheless, the company engaged in the distribution of phones through informal channels, as reported by Sky News (2020). Notably, instances have been documented wherein individuals with prior affiliations to law enforcement agencies or military entities were involved in the sale of these phones (Barnes, 2020). Law enforcement authorities contend that these devices witnessed widespread utilization within organized crime networks (Cox, 2020a). The French authorities first became aware of EncroChat phones in 2017, which led them to frequently seize such devices after numerous arrests within criminal organizations (Sky News 2020). Subsequently, these authorities discovered that the servers of this company were in France, prompting French authorities to engage in gaining access to this encrypted network.

The company behind EncroChat employed a cover company in Panama and an international bank account in Luxembourg for payment transfers. The company had a complete organizational structure with directors and employees in various countries, often playing fictitious roles to conceal the true purpose of the company. In the year 2022, the apprehension of eight individuals transpired, with three arrests taking place in Spain, three in Dubai, and the detention of a central figure, Paul KruSky, accompanied by his Canadian spouse, who was initially apprehended in the Dominican Republic but subsequently released under undisclosed circumstances (Daly & Cox, 2022). Concurrently, the encrypted communication platform Sky ECC emerged as a consequential counterpart after the operational disruption instigated by French, Dutch, and British law enforcement agencies against EncroChat in 2020 (Europol & Eurojust, 2020). Proclaiming itself as a prominent

entity within the domain of encrypted communications, Sky ECC purportedly boasted a user base exceeding 70,000 individuals. However, the company faced cessation following a security breach orchestrated by Belgian police in March 2021, paralleled by investigative endeavors initiated by U.S. authorities targeting its administrative figure.

The exploitation of compromised data from SKY ECC prompted Belgian law enforcement to execute raids in no less than 200 residential abodes, leading to the apprehension of a minimum of 48 suspects, including three legal professionals. Concurrently, Dutch authorities conducted searches in 75 residences, culminating in the arrest of 30 suspects and the seizure of weapons and 1.2 million euros in cash (Goodwin, 2021). The collective efforts of Belgian, French, and Dutch authorities, after the penetration of this communication application in 2021, afforded access to an expansive corpus of approximately 80 million messages (The Brussels Times, 2022). The meticulous analysis of these messages facilitated the initiation of around 276 novel investigations in 2022, encompassing 888 suspects, and resulted in the confiscation of over 90 tons of narcotics valued at 4.5 billion euros, in addition to the sequestration of cash and assets totaling 60 million euros (The Brussels Times, 2022).

In parallel with the trajectory of EncroChat, Sky ECC, established in 2008 by Jean-François Eap, operated transnationally from the United States and Canada. The company claimed high security, purporting protection from specialized eavesdropping like Pegasus. The company highlighted that encrypted messages were not stored on its servers, being destroyed immediately after reading within 30 seconds. If the user was unreachable and the phone was off, the sent message was stored for only 48 hours and then became irretrievable. Sky ECC phones were sold online or through authorized partners, with prices ranging from 900 to 2,000 euros, depending on the model, and were compatible with Android, Blackberry, and iOS systems. An additional enterprise providing encrypted communication through mobile devices was Ennetcom, an entity disbanded by Dutch authorities in 2016. The clientele of this service primarily comprised organized criminal elements operating within the Netherlands, amassing a subscriber base of 19,000 individuals. Interestingly, despite its Canadian origin, the company's servers were situated in Canada. The retail value of phones offered by Ennetcom was approximately 1,500 euros (The Guardian, 2016).

A similar phone to EncroChat, mainly used in the United States and Australia from 2008 to 2018, was Phantom Secure, with administrator Vince Ramos, a legitimate businessman. According to FBI investigations that led to Ramos' arrest in 2018, these phones were primarily used to facilitate the activities of drug traffickers. Criminal motorcycle gangs in Australia, known drug traffickers in California, and even members of the Sinaloa Cartel utilized such phones (Cox,

2020b). The company was legal and registered in Richmond, Canada, since 2008, initially considered a luxury phone and only used by VIPs for security reasons at its inception in 2008. However, over time, the services of this company fell into the hands of the criminal world. The company operated through an infrastructure outside of Canada, directing data through servers in Panama and Hong Kong to prevent accessibility by third parties (Cox, 2020b). The company provided customer services through call centers in Jalandhar, Punjab, India (Cox, 2020b). Phantom had domain addresses and registered companies in Bulgaria, Ireland, Singapore, and Thailand. Phantom sold around 7,000 to 10,000 phones primarily in Central and South America, Europe, the Middle East, Southeast Asia, and North America. Phantom phones allowed users to choose pseudonyms to hide their identity (Cox, 2020b).

Conversely, law enforcement agencies have actively devised encrypted platforms to ensnare criminal organizations and conduct covert surveillance on their activities. Referring to the US Embassy in Belgrade (2021, June 08), this is the case of the "ANOM" application, invested in by the FBI and Australian authorities. Starting in 201, ANOM managed to sell more than 12,000 encrypted devices used by at least 300 criminal organizations, including international drug trafficking organizations operating in more than 100 countries. Within just 18 months, the FBI, in the "Trojan Shield/Greenlight" operation, extracted over 25 million messages from members of various criminal groups discussing criminal affairs. Similar to WhatsApp, ANOM enabled encrypted conversations with text, photos, and videos. The application in question was pre-installed on mobile devices disseminated within the clandestine black market, typically accompanied by contractual agreements with annual fees reaching up to $4000. As corroborated by FBI assessments, a predominant concentration of ANOM users was discerned in Germany, the Netherlands, Spain, Australia, and Serbia (Farzan & Taylor, 2021).

Underworld cryptography: Balkan mafia and encrypted platforms

The adoption of encrypted communication platforms, exemplified by EncroChat and the SKY ECC application, has experienced a conspicuous increase in criminal activities carried out by groups originating from the European Union, the Balkans, and Great Britain. An exhaustive analysis conducted by the Global Initiative against Transnational Organised Crime (GITOC) substantiates the pronounced surge in the utilization of these platforms, notably during the period subsequent to 2021 (Risk Bulletin no.13, September-October 2022). According to the GITOC analysis, the number of SKY ECC users in Bosnia and Herzegovina is estimated to be around 2,500 subscribers (Risk Bulletin no.13, September-October 2022).

In December 2019, in Republika Srpska, 19 individuals were apprehended for drug and arms smuggling, communicating through SKY ECC. In April 2022, in Montenegro, former Chief Justice of the Supreme Court, Vesna Medenica, was arrested based on transcripts of communications between her son Milos Medenica and police officer Darko Lalovic, negotiating a drug shipment and cigarette contraband. According to Medenica, the judge was aware of these criminal activities and pledged assistance when required (Kajosevic, 2022).

Members of the criminal group led by Veljko Belivuk and Marko Miljkoviq, suspected of serious crimes including murder, were also found to have used SKY ECC. It is believed that their communications may have involved high-ranking officials and members of the state police. They were arrested in Belgrade in April 2022 (Risk Bulletin no.13, September-October 2022). A former high-ranking official in the Ministry of Internal Affairs of Serbia, Dijana Hrkaloviç, accused the Minister of Defense, Nebojsha Stefanoviç, of collaboration with certain media outlets presenting photos and videos of Danilo Vuçiç, the son of the Serbian president, Vuçiç, communicating with individuals from the criminal world through encrypted platforms. Hrkaloviç publicly accused Stefanoviç of supporting the criminal group led by Veljko Belivuk (Risk Bulletin no.13, September-October 2022).

As of April 2022, an excess of 100 individuals have been detained in Serbia, Bosnia and Herzegovina, Albania, Montenegro, and Slovenia, according to data provided by SKY ECC in collaboration with French and Dutch law enforcement agencies. These apprehensions were effectuated in connection with severe criminal transgressions, including but not limited to drug trafficking, homicides, and instances of forcible deprivation of liberty (Jeremic, Stojanovic, & Kajosevic, 2022).

Encoded modes of communication have become integral tools within the operational dynamics of Albanian criminal groups. In testimonial evidence related to contract killings, Nuredin Dumani delineates that communication and directives were effectuated through the utilization of "Matrix." (Gazeta Shqiptare, 2022). This platform, established by a non-profit entity registered in the United Kingdom, operates as an open protocol for internet communication and is recognized for its encrypted messaging application, "Element" (formerly known as "Riot"). Conceived with an emphasis on secure and private internet communication, Matrix adheres to open coding standards, providing a versatile range of communication modalities, encompassing encrypted messages, audio and video calls, group communication, and an array of other functionalities.

A notable illustration of the integration of encrypted communication platforms within the operations of Albanian criminal groups is evidenced in the case of Ardian Isufaj. Tasked predominantly as an intermediary between cocaine suppliers in South America and criminal markets in the European Union, Isufaj divulges

in intercepted communications with an Italian infiltrated agent. The disclosure unveils the strategic use of a secure phone, colloquially referred to as "Israeli," with features including non-interceptability, absence of a conventional number, and exclusivity for specified contacts. Isufaj asserts the dedication of this phone for the singular purpose of their criminal endeavors and introduces the term "Matrix" to describe its Israeli origin, emphasizing its 100% encryption (BalkanWeb, 2023).

Moreover, Albanian criminal entities have extensively employed applications such as SKY ECC and EncroChat-enabled phones. This utilization is conspicuous in significant investigations conducted by the Special Structure against Corruption and Organized Crime (SPAK) during the period 2019-2023. Notably, "Operation Metamorphosis" reveals the efficacy of encrypted conversations in identifying and pursuing the arrest of individuals associated with a prominent criminal organization in the Shkodra district. According to the SPAK press release (2023a, July 28), this conglomerate includes key figures such as influential businessmen, high-ranking state police officials, and a prosecutor in the year 2023.

A further achievement for SPAK emerges from a successful investigation wherein the decoding of encrypted conversations facilitated the identification and subsequent inquiry into a perilous criminal group in central Albania. Referring to SPAK press release SPAK. (2023b, January 2023), this group, responsible for attacking and injuring a prosecutor in 2019, led to the apprehension of six individuals, with four others subject to international search warrants.

Another significant case involves the dismantling of the "Kompania Bello" cocaine trafficking organization in September 2021. Dritan Rexhepi, considered the leader of this organization, was found to utilize encrypted communication platforms to engage in direct negotiations with South American drug cartels. The subsequent orchestration of an extensive network for transporting substantial quantities of cocaine from Ecuador to Europe involved collaboration with other group members operating in Italy, Holland, and Albania, as revealed by Europol (2020). Considering the widespread adoption of encrypted communication platforms by criminal groups in the Western Balkans, including Albania, the ensuing discourse presents a synthesized overview of jurisprudential stances emanating from some of the highest courts in EU member states and beyond.

Theoretical perspectives

Going back to the theoretical discussion, this article underscores the transformative impact of encrypted communication platforms, namely EncroChat and SKY ECC, on the investigation of organized crime. Several key theoretical perspectives emerge from the detailed examination of these platforms and their utilization

by criminal entities in the European Union, the Balkans, and Great Britain. It suggests a form of technological determinism, where the capabilities of encrypted communication platforms play a pivotal role in shaping the landscape of organized crime investigations. The advent of platforms like EncroChat and SKY ECC has not only facilitated sophisticated criminal activities but has also presented law enforcement agencies with unprecedented challenges. The encrypted nature of these platforms, with features such as non-traceability and swift data deletion, highlights the deterministic influence of technology on the strategies employed by organized crime groups and the subsequent adaptations required by investigative agencies (Lavorgna, 2016).

The digital criminology of coded forms of communication by organized crime notes the need for a paradigm shift in theoretical frameworks to accommodate the intricacies of crimes in the digital era. The integration of technology, particularly encrypted communication platforms, into the modus operandi of criminal organizations necessitates an updated criminological lens. Traditional distinctions between offline and online crimes are blurred, demanding a holistic understanding of the evolving dynamics within a digital society (Powell, Stratton & Cameron, 2018). The ramifications of EncroChat and SKY ECC extend beyond national boundaries, catalyzing the globalization of organized crime. The instances elucidated in the discourse encompass criminal activities that traverse multiple countries, necessitating synchronized endeavors among global law enforcement agencies. This corresponds with theoretical frameworks addressing transnational organized crime, underscoring the interlinked nature of criminal operations across borders and underscoring the imperative of international cooperation for efficacious counteraction against these threats (Leukfeldt, Lavorgna, & Kleemans, 2017).

The manifestation of criminal adaptation and innovation within organized crime is notably exemplified by the utilization of these communication platforms. Organized crime groups display a remarkable ability to adapt to technological advancements, leveraging encrypted communication platforms for their illicit activities. Simultaneously, law enforcement agencies are compelled to innovate in their investigative approaches, forming collaborations with technology providers and adapting to the changing landscape of organized cybercrime (Lavorgna & Sergi, 2016).

The instances observed within the Balkan Mafia elucidate a rapid assimilation of advanced encrypted communication tools, underscoring the notable adaptability of Albanian organized crime entities to dynamic technological landscapes. The purposeful utilization of platforms such as SKY ECC reflects a strategic imperative for safeguarding operational secrecy, thus highlighting a conscious integration of sophisticated communication technologies. These illustrative cases further manifest

instances of transnational collaboration facilitated by encrypted platforms, thereby providing tangible evidence of the expansive global outreach characterizing these criminal networks. Noteworthy is the strategic diversification represented by the adoption of multiple encrypted tools, a nuanced approach aimed at mitigating potential risks associated with compromise and infiltration.

On the other hand, the inherent adaptability of encrypted communication platforms to a diverse spectrum of criminal activities reveals a level of organizational sophistication within Albanian organized crime. The success of law enforcement in decoding these encrypted communications accentuates an enduring technological arms race, emblematic of the perpetual challenge authorities confront in maintaining pace with the technological advancements embraced by criminal enterprises. This dynamic underscore the pressing need for an adaptive and technologically proficient law enforcement framework in the face of evolving criminal methods of sophistication.

Finally, this is an area with a significant research deficit, which as this article highlighted is limited of the existing criminological theoretical frameworks in fully grasping the transformative ramifications of the digital society. The gap identified in theoretical frameworks highlights the need for critical reflection on the conceptual tools applied in understanding the complexities of organized cybercrime, urging scholars to revisit and adapt their approaches.

Conclusions

The integration of technology into criminal enterprises has undeniably blurred the traditional boundaries between physical and virtual dimensions of organized crime. This article has delved into the profound shifts brought about by the use of encrypted communication platforms such as EncroChat and Sky ECC by organized crime entities, revealing a critical gap in existing criminological theoretical frameworks. Our exploration underscores the urgent need for contemporary research hypotheses that can fully comprehend the transformative ramifications of these digital tools. While conventional distinctions between offline and online crimes have been extensively studied, the specific classification of advanced technological features employed by organized crime groups using encrypted communication platforms is notably absent.

Drawing on the evolving landscape described by Di Nicola as "digital organized crime," we propose an approach that transcends traditional and cyber contexts. Our focus centers on encrypted communication platforms like SKY ECC and EncroChat, serving as emblematic exemplars in the realm of organized cybercrime. This perspective challenges narrow and inflexible definitional paradigms,

emphasizing the need for a nuanced reconceptualization of fundamental concepts like extra-legal governance, violence, and territory.

The case studies of EncroChat and Sky ECC during the period 2019-2022 vividly illustrate the impact of such technologies on criminal activities. These platforms provided complete anonymity, non-traceability, and swift deletion of communications, facilitating organized crime on an unprecedented scale. The dismantling of these platforms by law enforcement agencies further highlights the dynamic interplay between technology and crime prevention.

On the other hand, this study sheds light on other instances such as Ennetcom, Phantom Secure, and the creation of encrypted platforms by law enforcement agencies like ANOM. These examples illustrate the dual role of technology in both enabling and countering organized crime. The global reach of these technologies, their intricate organizational structures, and the adaptability of criminal entities underline the necessity for a comprehensive and adaptive framework in understanding the sophistication of modern organized crime.

Furthermore, the case of Albanian criminal groups exemplifies the integral role of encrypted communication platforms within their operational strategies. The use of platforms like "Matrix" in contract killings and the strategic deployment of secure phones, such as the "Israeli" phone in cocaine trafficking operations, highlights the adaptability of criminal entities to exploit advanced communication technologies for their illicit activities. In essence, our contribution to scholarly discourse advocates for an inclusive perspective that encompasses the intricate dynamics of encrypted communication platforms. It encourages scholars and policymakers to move beyond outdated frameworks, recognizing the multifaceted nature of organized crime in the digital age. As technology continues to evolve, so must our understanding and methodologies to effectively combat and mitigate the impact of organized crime on societies worldwide.

References

Barnes, C. (2020, June 29). King con ex-soldier Johnny Swales 'sold encoded phones to crime gangs'. *Belfast Telegraph*. Retrieved in https://www.belfasttelegraph.co.uk/sunday-life/news/king-con-ex-soldier-johnny-swales-sold-encoded-phones-to-crime-gangs/39320873.html

BalkanWeb. (2023, October 11). Zbulohen përgjimet/ Agjenti italian u kamuflua si drejtor porti, ja si u arrestua shqiptari që trafikonte drogë nga Ekuadori. *BalkanWEB* in https://www.balkanweb.com/zbulohen-pergjimet-agjenti-italian-u-kamuflua-si-drejtor-porti-ja-si-u-arrestua-shqiptari-qe-trafikonte-droge-nga-ekuadori/#gsc.tab=0

Broadhurst, R., Grabosky, P., Alazab, M., & Chon, S. (2014). Organization and cybercrime: An analysis of the nature of groups engaged in cybercrime. *International Journal of Cyber Criminology*, 8(1).

Cox, J. (2020a, July 2). How Police Secretly Took Over a Global Phone Network for Organized Crime. *Vice* in https://www.vice.com/en/article/3aza95/how-police-took-over- encrochat-hacked

Cox, J. (2020b, October 22). The Network: How a Secretive Phone Company Helped the Crime World Go Dark. *Vice*. in https://www.vice.com/en/article/v7m4pj/the-network-vincent-ramos-phantom-secure

Daly, M., & Cox, J. (2022, June 29). Cops Investigating 'WhatsApp for Gangsters' Arrest Key Suspect in Caribbean. Paul Krusky played a crucial role in the development of encrypted phone firm EncroChat. Now he has been arrested in the Dominican Republic. *Vice*. in from https://www.vice.com/en/article/jgpqv4/encrochat-arrest-paul-krusky

Di Nicola, A. (2022). Towards digital organized crime and digital sociology of organized crime. *Trends in Organized Crime*. in https://doi.org/10.1007/s12117-022-09457-y

Dupont, B., & Whelan, C. (2021). Enhancing relationships between criminology and cybersecurity. *Journal of Criminology*, 54(1), 76–92. in https://doi.org/10.1177/00048658211003925

Europol. (2020, September 17). Joint investigation team leads to dismantling of one of Europe's most active Albanian-speaking networks trafficking cocaine into Europe. *Europol*. in https://www.europol.europa.eu/media-press/newsroom/news/joint-investigation-team-leads-to-dismantling-of-one-of-europe%E2%80%99s-most-active-albanian-speaking-networks-trafficking-cocaine

Europol & Eurojust. (2020, July 2). Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe. *EU Policy Cycle – Empact*. in https://www.europol.europa.eu/media-press/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe

Farzan, A. N., & Taylor, A. (2021, June 8). What is Anom, and how did law enforcement use it to arrest hundreds in a global sting? *The Washington Post*. in https://www.washingtonpost.com/world/2021/06/08/an0m-sting-faq/

Gazeta Shqiptare. (2022, May 20). Pas 'SKY ECC' vjen 'MATRIX'/ Si funksionon aplikacioni që përdorin grupet kriminale për t'iu shmangur përgjimit. *Gazeta Shqiptare*. in http://gazetashqiptare.al/2022/05/20/pas-sky-ecc-vjen-matrix-si-funksionon-aplikacioni-vrases-qe-perdoret-nga-grupet-kriminale-shqiptare-per-eliminuar-kundershtaret/

Goodwin, B. (2021, March 10). Police crack world's largest cryptophone network as criminal's swap EncroChat for Sky ECC. *Computer Weekly*. in https://www.computerweekly.com/news/252497565/Police-crack-worlds-largest-cryptophone-network-as-criminals-swap-EncroChat-for-Sky-NCC

Hamilton, F. (2020, July 3). Encrochat breach will make criminals wary. *The Times*. in https://www.thetimes.co.uk/article/encrochat-breach-will-make-criminals-wary3mzm3wc3q

Henry, N., Flynn, A., & Powell, A. (2020). Technology-facilitated domestic and sexual violence: A review. *Violence Against Women*, 26(15-16), 1828–1854.

Hughes, J. (2019, May 21). The £3,000 a year encrypted mobile phones with 'kill pills' being used by Gloucestershire drugs gangs. *Gloucestershire Live*. inhttps://www.gloucestershirelive.co.uk/news/gloucester-news/3000-year-encrypted-mobile-phones-2883942

Jeremic, I., Stojanovic, M., & Kajosevic, S. (2022, April 25). Encrypted Phone Crack No Silver Bullet against Balkan Crime Gangs. *Balkan Insight*. In https://balkaninsight.com/2022/04/25/encrypted-phone-crack-no-silver-bullet-against-balkan-crime-gangs/

Kajosevic, S. (2022, April 18). Montenegro Arrests Ex-Head of Supreme Court for Abuse of Office. *Balkan Insight*. In https://balkaninsight.com/2022/04/18/montenegro-arrests-ex-head-of-supreme-court-for-abuse-of-office/

Lavorgna, A. (2016). *Exploring the cyber-organised crime narrative: The hunt for a new bogeyman?* In P. C. van Duyne (Ed.), Organising fears, crime & law enforcement: New horizons and trends in Europe & beyond. Wolf Legal Publishers, Oisterveijk.

Lavorgna, A., & Sergi, A. (2016). Serious, therefore organised? A critique of the emerging "cyber-organised crime" rhetoric in the United Kingdom. *International Journal of Cyber Criminology*, 10(2), 170–187. in https://doi.org/10.5281/zenodo.163400

Leukfeldt, E. R., Lavorgna, A., & Kleemans, E. R. (2017). Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime. *European Journal on Criminal Policy and Research*, 23(3), 287–300. in https://doi.org/10.1007/s10610-016-9332-z

Mackenzie, S. (2022). Criminology towards the metaverse: Cryptocurrency scams, grey economy and the technosocial. *British Journal of Criminology*, 62(6), 1537–1552. https://doi.org/10.1177/1077801219875821

Powell, A., Stratton, G., & Cameron, R. (2018). *Digital criminology: Crime and justice in digital society*. Routledge.

Risk Bulletin no.13. (September-October 2022). Decryption of messaging app provides valuable insight into criminal activities in the Western Balkans and beyond. *Global Initiative Against Transnational Organized Crime*. in https://riskbulletins.globalinitiative.net/see-obs-013/01-decryption-of-messaging-app-criminal-activities.html

Saito, H. (2021, April 15). What Criminals Plan Via Encrypted Messaging Services, *InsightCrime*. in https://insightcrime.org/news/what-criminals-plan-via-encrypted-messaging-services/

Sky News. (2020, July 3). EncroChat: What it is, who was running it, and how did criminals get their encrypted phones? *Sky News*. in https://news.sky.com/story/encrochat-what-it-is-who-was-running-it-and-how-did-criminals-get-their-encrypted-phones-12019678

SPAK. (2023a, July, 28), Njoftim për shtyp, SPAK. in https://spak.gov.al/njoftimper- shtyp-date-28-07-2023/

SPAK. (2023b, January, 20), Njoftim për shtyp, SPAK. in https://spak.gov.al/njoftim- per-shtyp-15/

The Brussels Times. (2022, March 10). Operation Sky ECC: 888 suspects and €4.5 billion worth of drugs seized. *The Brussels Times*. in https://www.brusselstimes.com/justicebelgium/210112/operation-Sky%20-ecc888suspects-and-e4-5-billion-worth-of-drugs-seized

The Guardian. (2016, April 22). Dutch police Ennetcom shut down, owner arrested. *The Guardian*. in https://www.theguardian.com/world/2016/apr/22/dutch-police-ennetcom-shut-down-owner-arrested

U.S. Embassy in Belgrade. (2021, June 8). FBI Partners with Serbian Law Enforcement in Worldwide Operation Against Organized Crime. in https://rs.usembassy.gov/fbi-partners-with-serbian-law-enforcement-in-worldwide-operation-against-organized-crime/

Wall D. S. (2021). Cybercrime as a transnational organized criminal activity. In Allum F., Gilmour S. (Eds.), *Routledge handbook of transnational organized crime* (pp. 318–336). Routledge. 1–20.

Whelan, C., Bright, D., & Martin, J. (2023). Reconceptualising organised (cyber)crime: The case of ransomware. *Journal of Criminology*, 0(0). https://doi.org/10.1177/26338076231199793 Powell, A., Stratton, G., & Cameron, R. (2018). Digital criminology: Crime and justice in digital society. Routledge.