

From Chat to Crime: Telegram's Secrets!

Using a Mixed-Methods Approach to Decipher the Resilience of Telegram as an Illicit Market

Mennolt B. Verhaar



From Chat to Crime: Telegram's Secrets!

Using a Mixed-Methods Approach to Decipher the
Resilience of Telegram as an Illicit Market

By:

Mennolt B. Verhaar

4674685

in partial fulfilment of the requirements for the degree of

Master of Science

in Complex Systems, Engineering and Management (CoSEM)

at Delft University of Technology,
to be defended publicly on Monday March 17th, 2025 at 3:00 PM.

Supervisor:	dr. R.S. van Wegberg	TU Delft
Thesis committee:	dr. R.S. van Wegberg	TU Delft
	Prof. dr. M.E. Warnier	TU Delft
	ir. C.J. Volten	TU Delft

Executive Summary

Cybercrime has rapidly evolved into a global threat, facilitated by advancements in digital technology and the emergence of illicit online marketplaces. Among these, Telegram has become a key platform for criminal activity, offering an environment where illicit goods and services are traded with relative ease and anonymity. Its minimal content moderation, group and search functionalities have made it attractive for criminals. However, despite its increasing role in cybercrime, law enforcement struggles to effectively disrupt illicit activities, as traditional enforcement strategies face challenges to address the resilience and adaptability of such networks.

Despite extensive research on cybercrime, illicit Telegram marketplaces remain poorly understood, particularly in how they sustain resilience and adapt *modi operandi* despite enforcement. The role of automation and commoditisation in shaping these exchanges is largely overlooked, while reliance on outdated data limits insight into recent adaptive strategies. A community-centric approach is needed to examine marketplace dynamics, the impact of disruptions, and assess the impact of specified targeting on the adaptation of crime. This study answers these knowledge gaps by using the following research question: ***What ecosystemic mechanisms stimulate the resilience of Telegram as an illicit market?*** To answer this research question, a mixed-methods approach is used, where an extensive literature study and expert interviews are enriched with a large-scale data analysis with 1.4M independently sourced Telegram messages. These messages stem from 2021 to 2024 and are sent by 14,856 unique Telegram users in 45 Dutch Telegram channels. Using machine learning-based classification (SVM), topic modelling (LDA) and automated indexing, this study identifies *modi operandi*, payment preferences and patterns in communication. Ultimately, this research aims to uncover the systemic mechanisms driving adaptive cybercrime behaviours on Telegram by analysing the impact of automation, commoditisation, platform regulations, and law enforcement interventions. It examines how illicit markets sustain resilience, whether enforcement efforts lead to disruption or displacement, and how vendor specialisation and payment preferences shape underground economies. Thereby, this study provides insights to improve law enforcement strategies, inform policy development, and establish a scalable framework for future illicit ecosystems understandings.

The findings highlight automation and self-regulation as key factors in Telegram's resilience. Thereby, bots play a central role in message auto-deletion, channel moderation, scam detection, and mass message distribution, reducing exposure to law enforcement and increasing efficiency. Auto-deletion is widely used, with most channels setting messages to expire, effectively erasing digital footprints. The dataset shows that only 5.3% of messages are unique, a stark contrast to the 21.8% uniqueness rate in the reference dataset (2017-2021), underscoring the dominance of mass-distributed, repetitive advertisements. Additionally, vendors increasingly rely on outsourced advertising services, where intermediaries automate message forwarding across multiple channels (multi-homing), ensuring that criminal listings remain visible and accessible and minimising the impact of platform takedowns. This transformation shifts Telegram from a socially driven chat platform to an automated and heavily commoditised illicit marketplace.

Despite Telegram's recent increased moderation efforts, the study finds no empirical evidence of mass migration to alternative platforms. During the analyses, 33 channels ceased existence, resulting in only 38 of the 71 initially identified channels remaining active, indicating a deterrence effect, but no full elimination. This study further presents internal displacement mechanisms, such as invitation-based access systems and broadcasting channels for fast internal displacement.

Market specialisation primarily occurs at the vendor level, rather than the channel level. While channels present mixed products and services interchangeably, 67.6% of vendors specialise in offering a single crime category, whereas 32.4% engage in multi-category sales. Multi-category vendors display professionalism to an extent, as indicated by their broader range of accepted payment methods (1.63 on average, compared to 1.37 for single-category vendors). Furthermore, scarcity-driven demand is evident, observed in categories with fewer

advertisements, such as firearms and explosives, where user requests are more frequent. These observations suggest that law enforcement actions targeting specific markets do not eliminate demand but instead push buyers toward more proactive search behaviours. Besides, a shift in financial strategies is also observed. Cash has become the dominant payment method for drug-related transactions, replacing cryptocurrencies, likely driven by the physical nature of exchanges and pre-existing in-person contact. Cybercrime and financial fraud remain dominated by PayPal, Paysafecard, and cryptocurrencies due to their pseudo-anonymity and the online nature of the committed crimes. Last, a decline in Tikkie and bank transfers is observed, impacted by the traceability of these payments.

This study contributes to society and literature by revealing how Telegram has transformed into an automated, self-regulating and heavily commoditised illicit marketplace, challenging conventional views on cybercrime communities. It demonstrates that automation, self-regulation, and vendor specialisation drive market resilience, reducing reliance on social trust and replacing it with bot-driven enforcement mechanisms. Unlike assumptions that enforcement actions lead to cross-platform migration, findings suggest that crime displacement occurs within Telegram itself, facilitated by broadcasting channels and invitation-based access systems for wide automatic dispersion of invitation links. Additionally, the study uncovers scarcity-driven demand, where illicit products with limited supply generate increased user requests, shifting markets towards demand-based interactions rather than reducing crime. The commoditisation of services, including outsourced advertising and scam prevention, lowers barriers to entry, allowing even low-skilled actors to engage in cybercrime.

These insights provide a new perspective on digital illicit markets, emphasizing the need for enforcement strategies targeting the disruption of technological enablers in the ecosystem, namely automation, bot networks, and broadcasting channels, as these infrastructural mechanisms sustain illicit trade. Disrupting bots, scam registries, and invitation-based access can destabilise criminal networks. Instead of forcing criminals off Telegram, increased enforcement often pushes them towards demand-based interactions or into private invite-only spaces, (infiltration) strategies should therefore adapt accordingly. Besides, a differentiated approach is needed: casual users may be deterred through awareness campaigns, while professional criminals require direct disruption of their security measures. Proactive monitoring using Telegram's API by tracking high-risk keywords, administrator activities, and advertising patterns could provide real-time intelligence to disrupt criminal networks before they scale. For policymakers, legal clarity is needed on passive group membership and dual-use automation tools that enable crime. Strengthening regulatory frameworks and forcing providers to monitor misuse can curb illicit activities. Future research should focus on tracking internal crime displacement within Telegram, identifying central network hubs, and understanding how bot-driven automation influences illicit trade dynamics, including more research into the distribution techniques, executive actors, rates and the reach of these advertisements. Furthermore, future research can build on the applied methods and the intermediate outcomes, as it has some unresolved aspects. Last, establishing benchmark datasets will help track long-term market evolution and measure the true impact of enforcement measures.

Keywords: *Telegram, Resilience, Adaptation, Automation, Cybercrime, Bots, Self-Regulation*

Preface

With this thesis, I'm most likely concluding my academic journey. After my bachelor's and master's in Delft and Rotterdam, it's time to move on to the next phase of life and see where it takes me. Looking back at the past few months, I see a challenging yet rewarding period, with a topic that genuinely fits me, has kept me motivated from start to finish and allowed me to learn throughout the process.

Of course, things didn't go entirely smoothly. Before even starting with the actual research, my enthusiasm even got me banned from Telegram - something I can now laugh about. The ever-changing nature and relevance of this research topic made things tricky, too. Recent events such as changes to the platform's terms of service, the decision to share user data with authorities when requested and the effects of this, throughout this research added some extra complexity. Despite these challenges, I'm proud to have explored a world that feels far removed from daily life but, as I discovered, is surprisingly close if you know where to look - or if you randomly stumble across it while being curious. A funny one-liner (in Dutch) I came across unexpectedly and that has remained with me is: *'Met familie moet je wandelen, met vrienden moet je handelen!'*

Looking at the final result, I have to admit, I can say that I'm proud of what has been achieved in six months. The idea of digging into Telegram communities and uncovering how people operate, legitimately or otherwise, felt like a challenge worth taking. With somewhat limited Python skills, using quantitative methods I'd never tried before, through a lot of trial and error, and sometimes a little help from supportive people who were there when I needed them, it all came together.

I would like to express my gratitude to my supervisors for all their support throughout the process. Rolf, I'm truly glad I contacted you nearly a year ago and that you had such an engaging topic in mind. My fascination with this subject was sparked five years ago during one of your guest lectures and I'm glad to conclude this master with you. Thank you for your wild ideas, your insights, and the enjoyable meetings over good *'brandstof'* (coffee). Cécile, thank you for all the encouragement and support during our weekly meetings, the laughter, and the fact that I could always stop by. Martijn, I appreciate your insightful and constructive feedback throughout the process, such as the assistance in reflecting on the reasons behind the question.

Moreover, I want to take a moment to thank those who have been important to me during my thesis. Stiene, my family, Jip and my housemates, Pepijn, Sybe and Bart, thank you all for your support! If I needed to brainstorm, had technical (*Python!*) questions or just wanted to chat, I knew I could always turn to you. I can imagine that, at times, I might have asked questions with more obvious answers, but thank you for always being there and your willingness to help. Lastly, I wouldn't say that writing this thesis has been an easy journey, but being surrounded by supportive peers at TPM has made it much more manageable. Thank you to everyone who played a part in this journey.

Enjoy the reading! Hopefully, this topic sparks the same enthusiasm in you.

M.B. Verhaar
Delft, March 2025

Table of Contents

Executive Summary	iv
Preface	vi
1 Introduction	1
1.1 Relevance and Contributions	2
1.2 Report Outline	3
2 State-of-the-art	4
2.1 Background	4
2.1.1 Communities: Marketplaces and Forums	4
2.1.2 Platform Migration	6
2.1.3 Data-Driven Enforcement and Research	7
2.2 Research Gaps in Current Literature and Practice	8
3 Research Design and Methodology	10
3.1 Research Objective	10
3.2 Research Questions	11
3.3 Methodology	11
3.3.1 Rationale for Qualitative Analyses	11
3.3.2 Rationale for Quantitative Analyses	13
4 A Theoretical Lens on Adaptation and Resilience in Illicit Markets	19
4.1 Exploring the System Environment	19
4.1.1 Law Enforcement	19
4.1.2 Technology and Innovation	21
4.1.3 Social Ties	21
4.1.4 Demand, Important Events & Media	22
4.2 Consequences and Impact on Criminal Behaviour	23
4.2.1 Community Closure	23
4.2.2 Crime Displacement	24
4.2.3 Commoditisation & Fragmentation	25
4.3 Conclusion	26
5 Setting the Context	27
5.1 Use of Telegram	28
5.2 Modi Operandi	28
5.2.1 Demand Identification and Recruitment	29
5.2.2 Knowledge Level and Dissimilation of Expertise	29
5.2.3 Conventional Payment Methods Observations	30
5.3 Conclusion	31
6 Detailed Quantitative Approach	33
6.1 Scraping: Telethon API	33
6.2 Labelling and Classifying: Annotation and Support Vector Machines	35
6.3 Topic Modelling: Latent Dirichlet Allocation	40

6.4	Finding Payment Methods: Automated Message Indexing	43
7	Operational Trends & Patterns	44
7.1	Automation and Self-Regulation	44
7.1.1	Message Auto-Deletion	44
7.1.2	Commoditisation of Message Distribution	45
7.1.3	Channel Moderation	46
7.2	Views, Shares & Contributors	48
7.3	Channel (In)continuation	49
7.4	Channel and Vendor Specialisation	50
7.5	Conclusions	52
8	Discussion	54
8.1	Placing the Trends in Context	54
8.1.1	Telegram's Transformation from Messaging Service to Heavily Commoditised Market	54
8.1.2	Dynamic Displacement within Telegram	56
8.1.3	Vendor and Channel Specialisation	57
8.2	Limitations	57
8.2.1	Limitations in the Qualitative Approach	57
8.2.2	Limitations in the Quantitative Approach	58
8.3	Reflection & Future Research	60
8.4	Recommendations	61
9	Conclusion	63
	References	65
	Appendix A: Interview Protocol	72
	Appendix B: Telegram Market Descriptives	73
	Appendix C: Referenced Messages	75
	Appendix D: Confusion Matrices	76
	Appendix E: LDA Addendum	77
	Appendix F: Payment Methods Addendum	82

List of Figures

Figure 1: Example Telegram Advertisement: (Dutch) Ad for Hard Drugs	6
Figure 2: Research Process Diagram	33
Figure 3: Message Types per Channel	39
Figure 4: Advertisement Categories per Channel	40
Figure 5: Coherence Scores for Chat Messages (left) and Bot Messages (right)	42
Figure 6: Message Distribution over Time	45
Figure 7: Unique Messages per Message Type	45
Figure 8: Total and Unique (Offer) Advertisement Sent per Vendor	46
Figure 9: 'Share to Unlock' and 'Join All Channels'	46
Figure 10: Message Views (upper) and Shares (lower) Boxplot	49
Figure 11: Product Range Specialisation	51
Figure 12: Offer and Request Distribution per Category	52
Figure 13: Most Frequent Sent (Identical) Message	75
Figure 14: Message containing 'SEO tags'	75
Figure 15: Request Message for Money Mules	75
Figure 16: Message Types Confusion Matrix	76
Figure 17: Advertisement Category Confusion Matrix	76
Figure 18: Chat Message Topics	77
Figure 19: Bot Message Topics	79
Figure 20: Coherence Scores for Reference Dataset (2017-2021)	80
Figure 21: Chat Message Topics (2017-2021)	81
Figure 22: Missed Payment Indicators per Added Signal Word	82
Figure 23: Payment Preference per Ad. Category and Overall Distribution	83
Figure 24: Heatmap: Relation between Ad. Category and Preferred Payment Method	84
Figure 25: Heatmap: Relation between Ad. Category and Preferred Payment Method (2017-2021)	84
Figure 26: Uniquely Accepted Payment Methods per Vendor Type	85

List of Tables

Table 1: Interview Respondent Overview	27
Table 2: Comparison of Descriptive Statistics between Current Dataset and Reference Dataset	34
Table 3: Available Message Types with Example Text	35
Table 4: Available Advertisement Categories, adapted from Boersma (2023)	36
Table 5: Manually Labelled Types & Category Distribution	37
Table 6: Unique Messages per Message Type in Current Dataset and Reference Dataset	40
Table 7: Telegram Channel Overview and Descriptives	74
Table 8: Currencies Wordlist	82

1 Introduction

In today's digital age, cybercrime has become a pervasive global threat, driven by rapid technological advancements and the emergence of online illicit marketplaces. Platforms such as Telegram, a cloud-based messaging service originally designed for secure communication, have evolved into key enablers of cybercriminal activity. With its minimal content moderation, large-group functionalities, and anonymity features, Telegram has become an *offender convergence setting*, where criminals trade illicit goods and services, exchange expertise, and coordinate operations (Garkava et al., 2024; Leukfeldt et al., 2017, p. 1389; Paquet-Clouston & García, 2022). The issue is not minor in scale. Law enforcement agencies and researchers increasingly report widespread criminal trade on Telegram, spanning drug sales, financial fraud, hacking services, and counterfeit documents. A recent study found over 2.5 million drug-related advertisements across 21 Dutch Telegram groups, demonstrating the platform's role in facilitating cybercrime at scale (NOS, 2024). Unlike traditional dark web markets, which require technical expertise and anonymity tools such as Tor and cryptocurrencies, Telegram offers a low-barrier alternative, making it highly attractive to both seasoned cybercriminals and opportunistic offenders (Hutchings, 2014). Its accessibility is further improved by automation tools, allowing illicit actors to efficiently scale their operations.

Structurally, Telegram consists of channels, where administrators broadcast messages to subscribers, and groups, where all members can engage in discussions. In criminal contexts, these communities function as dynamic illicit marketplaces, with vendors advertising their services, buyers seeking goods, and administrators using Telegram's (automating) functionalities to sustain operations despite enforcement pressures. Throughout this study, the terms channels, groups, communities, and marketplaces are used interchangeably, reflecting their overlapping roles. Given Telegram's widespread use in the Netherlands and its role in facilitating crime, this research focuses exclusively on Dutch Telegram communities (Roks & Monshouwer, 2020). By analysing illicit activity within these groups, key insights can be gained into how cybercriminal networks function, adapt and sustain their operations over time.

Despite law enforcement efforts to disrupt these digital illicit economies, criminals consistently outpace interventions, demonstrating a remarkable capacity for adaptation and resilience (Roy et al., 2024). This persistent challenge is often described as a cat-and-mouse game, in which enforcement actions trigger crime displacement, where illicit activities do not disappear but rather shift in form, migrate or evolve through alternative operational methods (Ladegaard, 2020). As a result, traditional enforcement strategies are frequently ineffective in achieving long-term disruptions (Ladegaard, 2019; Ouellet et al., 2022). Telegram exemplifies this issue. Despite increased moderation efforts and channel takedowns, it remains a resilient hub for cybercrime. But why does this platform continue to thrive despite enforcement efforts? The mechanisms enabling its persistence remain poorly understood, particularly how criminal actors maintain operational continuity, the structural and organisational strategies that sustain illicit networks, and the role of automation and specialisation in shaping these evolving marketplaces.

Existing research has primarily focused on individual crimes, such as drug trafficking, fraud, and hacking, without addressing the broader systemic mechanisms that enable illicit marketplaces to persist and adapt (Kruisbergen et al., 2019). However, cybercriminal markets do not operate in isolation; they function as interconnected ecosystems where technological, operational, and community-driven mechanisms interact to ensure resilience (Baraz & Montasari, 2023). The role of automation and vendor specialisation in shaping efficiency, as well as commoditisation strategies that standardise and outsource illicit offerings, remains largely unexplored in the context of Telegram communities. Insights in the methods in which commoditisation is offered gives great insights into the level of barriers to entry these markets and the range of actors that participate. Furthermore, the rapid shifts in criminal behaviours and *modi operandi* are not well captured due to a reliance on outdated datasets, especially since Telegram criminals increasingly adopt new techniques such as automation and encrypted communication (Boekhout et al., 2024). Understanding the enabling dynamics, and the impact on displayed adaptive *modi operandi*, is critical for law enforcement and policymakers, as it enables a shift of focus from reactive interventions, such as

shutting down individual channels, to proactive disruption strategies that target the underlying enablers of criminal continuity and can potentially be applied in underground communities besides Telegram.

The objective of this research is to uncover the ecosystemic mechanisms that sustain the resilience of Telegram as an illicit marketplace. By using a mixed-methods approach, this study uses cybercrime concepts as a theoretical lens to analyse empirical insights, derived from Dutch independently sourced Telegram communities. Therefore, first, mechanisms that drive behavioural adaptation within communities are identified, such as automation, commoditisation and specialisation. These are used to establish a theoretical framework to interpret the structural enablers of resilience within Telegram's criminal ecosystem. Succeeding, operational and technological strategies used by illicit actors are empirically determined, from a community-level perspective, instead of taking a vendor-level viewpoint.

Specifically, this research aims to investigate how users and administrators leverage technological tools to structure and sustain criminal channels, identify the mechanisms that facilitate market continuity despite enforcement efforts, and research the role of vendor and channel specialisation in maintaining communities' adaptability. By combining these approaches, this study provides a data-driven understanding of Telegram's evolving illicit economy, offering valuable insights for law enforcement and policymakers to develop more targeted, proactive interventions to destabilise networks at scale, while advancing academic understanding of the driving mechanisms behind community dynamics and resilience. Additionally, it establishes a reproducible methodology for future research, enabling longitudinal tracking of the displayed *modi operandi* in communities, understanding the adaptive application of ecosystemic mechanisms and the effectiveness of enforcement strategies over time. Although the depicted scenario is closely tied to international communities, it is essential to be able to present recommendations that are fully applicable and executable within the Dutch jurisdiction of law enforcement agencies, therefore, this research only targets Dutch Telegram communities.

1.1 Relevance and Contributions

The societal relevance of this research lies in addressing the broad spectrum of crimes facilitated by platforms like Telegram, including cybercrime, drug trafficking, weapons dealing, fraud, and money laundering. The urgency to address this situation stems from the widespread societal harm caused by these activities, including financial losses, public health crises, and the erosion of trust in digital ecosystems. By identifying the key drivers behind criminal adaptation, contextualizing these trends, and developing more effective strategies for law enforcement and policymakers, society can be made more resilient by reducing the prevalence and harm of the exchanged criminal products and services. Overall, this research:

- Provides a detailed (quantitative) snapshot of the illicit Telegram ecosystem, offering insights into:
 - o Operational tactics, including vendor specialisation, shifting payment preferences, and risk mitigation strategies.
 - o Automation, commoditisation, and professionalisation strategies, showing how criminals exploit bots, self-regulating mechanisms, and legitimate tools to innovate and scale illicit activities
 - o Communication dynamics, showing how criminals interact, advertise, coordinate illicit activities.
- Demonstrates mechanisms enabling crime displacement within Telegram, showing that enforcement efforts lead to internal migration rather than platform abandonment by showing the role of gatekeeping systems and broadcasting hubs.
- Contextualises criminological theories to the Telegram ecosystem, bridging gaps between research on traditional online crime (dark web) and Telegram-based illicit activity.
- Establishes a scalable data-driven and reproducible approach for future studies, serving as a benchmark for analysing the broader evolution of Telegram as an illicit market.

This research spans multiple domains, including policy and management, governance and regulation of complex societal issues, and technology, making it a highly relevant topic for a master's thesis in Complex Systems

Engineering & Management (CoSEM). Its relevance to CoSEM is highlighted by three key facets. First, it examines the interdependencies between criminal activities, legislation, innovation, and platform regulation. Second, it emphasises multi-actor management, involving platform users, law enforcement agencies, Telegram (as platform provider), regulatory bodies, and the general public. Lastly, it applies systems thinking and data-driven decision-making, using independently sourced and labelled data to analyse Telegram's illicit ecosystem.

1.2 Report Outline

This research is structured as follows. Chapter 2 presents a brief literature review, outlining existing research on Telegram's role in cybercrime. Chapter 3 presents the objective of this research based on the found knowledge gaps, the utilised research questions and the rationale behind the chosen methods. Chapters 4 and 5 dive deeper into Telegram's system characteristics and criminal ecosystem by drawing parallels with dark web marketplaces, and contextualising the concepts through expert interviews. Chapter 6 describes the detailed technical approaches for data collection and analysis, covering scraping, classification, and topic modelling methods. Chapter 7 presents the observed trends, originating from the quantitative findings, with insights related to the 45 analysed Telegram groups, its users, discussion topics from chat and bot messages and insights into preferred payment methods. Chapters 8 and 9 conclude the study by discussing its contributions, limitations, and final conclusions.

2 State-of-the-art

2.1 Background

Cybercrime, broadly defined as criminal acts conducted through or directed at computer systems, can be divided into two main categories: *cyber-enabled crime*, which includes offences such as hacking and malware distribution, and *cyber-assisted crime*, where the internet facilitates traditional criminal activities, such as drug trafficking (Beerthuizen et al., 2020; European Commission, n.d.; Van Wegberg, Oerlemans, et al., 2018). While many studies focus on either traditional crime or cybercrime, Kruisbergen et al. (2019) emphasise that modern technology increasingly influences traditional criminal organisations. It offers new opportunities for criminals to communicate, recruit, and operate in ways that were previously impossible, such as through the use of encryption or online forums (Bijlenga & Kleemans, 2018). Traditional organised crime, such as drug trafficking and human smuggling, continues to take place in the physical world. This trend highlights the connection between online and offline criminal activity, as digital tools facilitate transactions that have significant real-world consequences (Van Wegberg, Tajalizadehkhoob, et al., 2018). The continuous shift of displayed crime types and used payment methods, aggregated in the term *modi operandi*, complicates the effectiveness of law enforcement interventions. *modi operandi* refer to the habits of working of a set of individuals or an aggregated group, e.g. the methods of operation such as the offered crime types, the used payment methods, the relation between these and the undertaken approaches to offer these illicit services or products.

The behaviour of users in illicit Telegram marketplaces has received limited attention in existing research. To avoid overlap with previously conducted studies, first, environments that share similar characteristics as Telegram are identified and parallels are drawn. By exploring key differences between these underground marketplaces and forums, highlighting recent developments within Telegram and exploring methods of data-driven research and enforcement, research gaps can be established.

2.1.1 Communities: Marketplaces and Forums

Underground communities serve as platforms for illegal activities, including drug sales, fraud, and the exchange of cybercrime tools and services. By using online communities, perpetrators can reach a wider array of victims than what is feasible through traditional, physical criminal activities (Hutchings, 2014). Cybercrime communities can be categorised into two main types: those on the *dark web* and those on the *surface web*, distinguished by their levels of anonymity and accessibility. The dark web, inaccessible via standard browsers, is home to more private and illicit activities, whereas surface web forums, though less anonymous, still facilitate discussions about illegal goods (Cabrero-Holgueras & Pastrana, 2021; Hughes et al., 2024). Hou et al. (2022) further categorise communication on these platforms into four distinct levels. The first layer consists of open forums and marketplaces, like those found on the dark web, which provide a degree of anonymity while remaining accessible with minimal barriers. In contrast, the second and third layers are more exclusive, consisting of smaller, invitation-only groups. At the core of these layers are offline networks that organise large-scale cybercrime operations. Telegram, which can offer encryption, used to be minimally regulated and is particularly popular among cybercriminals, exhibits a hybrid model, sharing some characteristics with open dark web marketplaces (level 1) and exclusive cybercrime networks (level 2 and 3) (Hou et al., 2022; Hughes et al., 2024).

Such platforms function as *offender convergence settings*, where criminals gather to trade goods and services, discuss techniques, and share knowledge, which facilitates the rapid dissemination of criminal expertise, making these communities essential to the growth of cybercrime networks (Leukfeldt et al., 2017, p. 1389; Paquet-Clouston & García, 2022). Some communities are invite-only, limiting participation to trusted individuals, which not only restricts access but also poses challenges for researchers seeking to enter these groups (Hughes et al., 2024). To understand why Telegram is widely used among criminals, it is essential to first gain a better understanding of darknet marketplaces and forums and to use a comparative lens with Telegram marketplaces.

Darknet Marketplaces

Darknet marketplaces (DNMs), or *crypto markets*, function like e-commerce platforms but specialise in illegal goods and services. Listings are organised into categories with searchable products, vendors, and departments, featuring descriptions, images, and customer reviews (Armona, 2018; Hughes et al., 2024). Users often switch between buyer and seller roles, guided by administrators who set policies and moderators who detect fraud (Basheer, 2022; Jardine, 2021). Compared to traditional drug markets, DNMs eliminate intermediaries, reducing costs and increasing profitability for participants (Demant et al., 2018).

Underground marketplaces, do not directly sell products but instead function as platforms or intermediaries that provide an environment for illegal transactions (Soska & Christin, 2015). Some vendors specialise in selling a single product, while others offer a range of items. However, most vendors tend to operate on a smaller scale, with only a few achieving substantial financial success, with the majority of vendors earning less than \$10,000 throughout their entire operational period (Soska & Christin, 2015). Nevertheless, as van Wegberg et al. (2020) emphasise, these platforms significantly lower the entry barriers for cybercriminal entrepreneurs and offer structured data on trades and reputations, as listings must be formatted systematically and efficiently. In the final stage of illegal transactions, often referred to as *the last mile*, where vendors and buyers (virtually) meet and exchange goods, consumers rely heavily on vendor reputation due to the inability to assess product quality or vendor credibility beforehand (Schrama et al., 2022). This trust is built in, and protects both vendors and buyers during transactions, by including dispute arbitration and customer and vendor feedback systems with written reviews (Armona, 2018; Barratt & Aldridge, 2016; P.-Y. Du et al., 2018). Additionally, escrow services, where payments are held by a third party until both buyer and seller are satisfied, reduce financial risks (Hutchings, 2014; Jardine, 2021). Cryptocurrencies and anonymity protocols further shield users from law enforcement, while the absence of physical interaction minimises the risk of violence (Soska & Christin, 2015; Verburch et al., 2018). Notably, these safety mechanisms were not initially developed for illegal activities but were adapted from legitimate online commerce practices (Aldridge & Decary-Hetu, 2015). As users' identities and locations are hidden through the TOR protocol, it is nearly impossible for law enforcement to trace individuals, protecting individuals from identification and prosecution (Armona, 2018).

Cybercrime Forums

Cybercrime forums, such as Dread, whether on the dark or surface web, serve as convergence points for criminals. These platforms are typically organised into structured threads and subforums, where users discuss criminal tactics, trade illicit goods, and exchange knowledge (Boekhout et al., 2024; Hughes et al., 2024). The structured nature of these forums facilitates communication and trust-building among participants, both of which are essential for successful criminal operations. Each forum thread typically begins with an initial post introducing a new topic, followed by replies that contribute to the discussion or provide solutions to specific issues (Hughes et al., 2024).

Telegram

Darknet marketplaces have existed for a longer time, resulting in more extensive research on these platforms. Although these marketplaces exhibit numerous differences (such as structure), they also share certain similarities. Therefore, a comparative lens is used to gain deeper insights into Telegram's role and functionality.

Telegram functions as an underground marketplace and criminal communication channel simultaneously, providing the best of the two worlds. Within Telegram, channels function as one-way communication from administrators to followers, whereas groups function like other group chats. Vendors and customers use (open) groups to offer illegal products and services and to talk freely amongst themselves, without the strict structure typically seen in darknet marketplaces (P.-Y. Du et al., 2018; Hughes et al., 2024). There is more resemblance in the fact that these marketplaces also have a group owner and often use moderators, which can be the same person. Besides, users can often switch between the vendor side and the buyer side of a deal. The groups, however, appear considerably more chaotic due to a lack of established structure, and because users determine the structure of their chat messages independently, from which a real (anonymised) example is shown in Figure 1. Furthermore, there are no mechanisms in place to foster trust (such as dispute arbitration or escrow services).

Telegram has become a favoured tool for cybercriminals due to its ease of use, its possibility for end-to-end encryption, and minimal regulation. While this end-to-end encryption is optional and needs to be selected in one-on-one conversations, this feature is not available for groups or groups. However, it does have the status of secure messaging, partly due to the capability to create large, anonymous groups which made it highly attractive for illicit activities. Criminals use Telegram to sell illegal products, including drugs and weapons, distribute malware, and trade stolen data, using channels and groups as marketplaces or forums for discussions. Recent research by Roy et al. (2024) identified 339 Telegram groups containing illicit activities, which were followed by 23.8 million users. A detailed examination of the content revealed that more than 28% of the URLs shared were linked to phishing attacks, while 38% of the shared files contained malware. During the research period, it was estimated that Telegram had 900 million users globally (Statista, 2024), providing an indication of the scale of illicit activities taking place on the platform.

Telegram groups tend to be more open and require minimal registration, with users often being less cautious about protecting their anonymity. Access is considerably easier compared to dark web marketplaces, as there is no requirement for knowledge of Tor. Furthermore, one only needs to know the name of a group or make an educated guess to view public groups through a straightforward chat interface. In contrast, dark web forums are generally more secure, frequently requiring invitations or advanced authentication methods, reflecting the higher sensitivity of the activities discussed in these spaces (Cabrero-Holgueras & Pastrana, 2021).

2.1.2 Platform Migration

Telegram has recently emerged as an underground community, with a few factors that have attracted criminals to these new grounds. These exhibited adaptive behaviours are shaped by both external pressures and internal dynamics, influenced by technological, regulatory, and systemic changes. These adaptive strategies mirror trends observed in other illicit marketplaces, such as those on the dark web, and highlight the resilience of these networks.

Criminal activities on Telegram are heavily influenced by regulatory changes and law enforcement interventions. Recent operations, such as Operation SpecTor, have demonstrated the potential for short-term disruption in criminal marketplaces. These interventions, including the seizure of goods and the shutdown of platforms like Monopoly Market, temporarily destabilise criminal ecosystems (Politie, 2023). Similarly, Dutch law enforcement has recently targeted the exchange of personal data on Telegram, a practice that facilitates broader criminal activities (Politie, 2024). These enforcement efforts are crucial as they disrupt market dynamics temporarily and force criminals to adapt their strategies. However, evidence from dark web marketplaces suggests that such interventions yield limited long-term effectiveness. Studies show that markets typically recover quickly, with trade volumes often returning to pre-takedown levels or even exceeding them, which could be due to increased visibility from media coverage (Décary-Héty & Giommoni, 2017; Ladegaard, 2019; Ouellet et al., 2022). It is therefore argued that taking down marketplaces yields short-term outcomes; however, it is arguably insufficient for sustainable effectiveness in the long term, as individuals are capable of adapting and reorganising (Ladegaard, 2019). In literature, reorganising

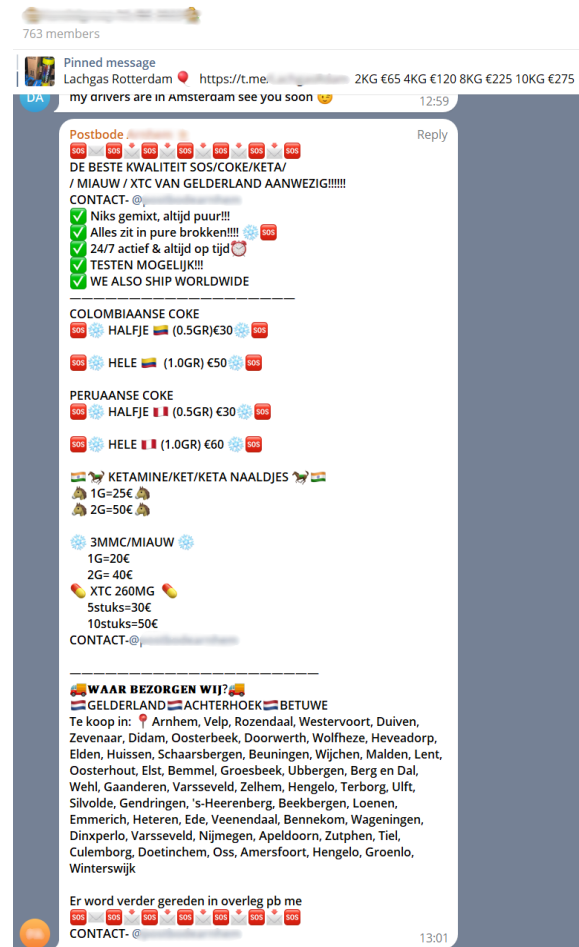


Figure 1: Example Telegram Advertisement: (Dutch) Ad for Hard Drugs

at other platforms is known as crime displacement or the waterbed effect, which involves a shift in criminal activities from one platform to another rather than full elimination (Moeller et al., 2017; Ouellet et al., 2022; Verburgh et al., 2018). Criminals adapt by cross-listing goods on multiple platforms or migrating to encrypted platforms like Signal or invite-only dark web environments, reducing their vulnerability to single-platform shutdowns.

Telegram's recent announcement to share phone numbers and IP addresses with authorities marks a significant platform change (Roy et al., 2024; Wokke, 2024). While the long-term implications remain uncertain as this announcement is very recent, it is evident that criminals remain vigilant due to this change.

A key driver of adaptive behaviours on Telegram could be related to the commoditisation of cybercrime. The rise of Cybercrime-as-a-Service has lowered barriers to entry, allowing individuals with limited technical expertise to participate in sophisticated criminal operations and to quickly adapt to enforcement efforts and new opportunities (Akyazi et al., 2021; Manky, 2013; Van Wegberg, Tajalizadehkhoob, et al., 2018). Telegram's (former) lack of content moderation and ease of connecting with buyers make it an attractive platform for discovering new markets and outsourcing operations. Specialised tools, such as malware kits and cash-out services, are readily available, enabling criminals to focus on networking rather than technical skill development (Kruisbergen et al., 2019).

Besides the displayed adaptive behaviours for platform choices, preferences for payment methods move along. The reliance on virtual currencies has emerged as a critical enabler for outsourced criminal activities. Cryptocurrencies, with their semi-anonymous nature, decentralised control and the fact that they are unregulated by central banks, means that they are particularly well-suited for the financial transactions that sustain the cybercrime economy (Kruisbergen et al., 2019; Schrama et al., 2022). Criminals employ these currencies in their cash-out strategies, by laundering money through a series of cryptocurrency transactions to hide its origins (Van Wegberg, Oerlemans, et al., 2018). Research conducted by Kruisbergen et al. (2019) revealed that cryptocurrencies have facilitated drug dealing and malware distribution, making it easier for criminals to evade law enforcement. However, traditional payment methods, such as cash, continue to dominate in offline organised crime, with some criminals also using newly developed payment methods like prepaid credit cards.

2.1.3 Data-Driven Enforcement and Research

Law enforcement agencies (LEAs) face considerable challenges in addressing the evolving landscape of cybercrime. Criminals continuously find new ways to exploit technology to evade detection, meaning that the *modi operandi* are in a continuous shift. By examining the roles of law enforcement and research, it is possible to identify knowledge gaps within the ongoing cat-and-mouse dynamic of combating cybercrime.

Identifying novel *modi operandi* has become more feasible for three reasons: (I) the increased use of virtual currencies, which are more public by design and allow for improved transaction tracking, (II) criminal activities are now more frequently discussed and transacted in public or more accessible communities (e.g. Telegram), and (III) underground marketplaces tend to collect more data about their users and transactions (Aldridge & Askew, 2017; D. Y. Huang et al., 2018). Transactions and discussions that were once private now occur in public spaces, as vendors and buyers have gained a greater sense of security and confidence (Schrama et al., 2022). Understanding the flow of funds through large-scale data analysis has become essential for generating insights from underground communities (Beerthuizen et al., 2020; Schrama et al., 2022).

Traditional law enforcement in the Netherlands is mainly reactive at the same time, often addressing crime only once detected rather than disrupting criminal networks proactively (Schrama et al., 2022), resulting in crime displacement in the long term (Ladegaard, 2019; Ouellet et al., 2022). Furthermore, law enforcement struggles with decentralised, anonymised systems, where investigations usually start only after clear indicators of crime are present, potentially missing criminal trends (Interpol, 2022; Schrama et al., 2022). Limited resources are spent on broader criminal phenomena, focusing instead on individual cases. Experts argue that phenomenon research could provide valuable insights into the allocation of enforcement capacity. Insights gained from phenomenon research

can help law enforcement keep pace with the rapid developments in virtual currencies, which are constantly evolving. Thus, there is a strong need for more efficient, data-driven enforcement strategies that use recent data.

Research into these phenomena varies in scale, with some studies examining trends, developments, and the size of underground communities (Verburgh et al., 2018). Large-scale investigations often gather data through methods such as web scraping, undercover participation, or analysis of data retrieved during law enforcement interventions. Other researchers focus on case studies, which have found, for example, that virtual currencies are frequently linked to money laundering schemes (Leuprecht et al., 2022). However, due to the specific scope and the focus on particular languages or regions, such studies may have limited generalizability.

According to Hughes et al. (2024), research on the cybercrime community can be categorised into eight distinct objectives, although it is important to note that individual research articles may address several of these goals concurrently. Some important and recent categories are:

- *Key Actor Detection.* Through analysis, players that fulfil a central node function in underground communities are found, based on their reputation or on the number of transactions that they play a role in. Key actors are characterised as individuals engaged in activities that attract the attention of law enforcement. This includes criminal behaviours, such as the distribution of hacking tools, but also actions that, while not inherently illegal, could potentially result in future offences (Hughes et al., 2019).
- *Discourse Analysis.* Discourse analysis focuses on the future, by examining the specific jargon and language utilised on platforms (Hou et al., 2022; Hughes et al., 2020; Macdonald et al., 2015) and by investigating emerging forms of criminal activity on these platforms through automated methodologies (such as Machine Learning) (Deliu et al., 2018).
- *Crime Type.* Cybercrime communities enable a range of illicit activities, categorised under various crime types. Understanding the various crime types is important in order to promote targeted law enforcement on these platforms (Schrama et al., 2022). Much attention in this type of research is paid to cybercrime (malware distribution) or illicit products and/ or services (Durrett et al., 2017; Macdonald & Frank, 2017).
- Other studies aim to analyse forums over a longer time (*longitudinal*), forum descriptives (such as the number of posts, vendors and transactions), aim to understand the underlying economies in platforms (*economic*) or use Machine Learning to discover information about cyber-attacks (*cyber threat intelligence*) (Akyazi et al., 2021; Hughes et al., 2024; Kühn et al., 2024; Motoyama et al., 2011).

When examined over time, certain research objectives are pursued with greater frequency than others. For instance, the economic aspects of platforms receive less focus, whereas longitudinal and discourse analyses have gained significant attention over the years (Hughes et al., 2024). Research into crime types has varied strongly over the past few years. In general, the number of publicised articles using quantitative research methods has increased strongly since 2016. These methods of research result in various novel insights about underground communities. In a recent longitudinal study conducted by Schrama et al. (2022), with the objective to investigate the use of virtual currencies in primarily financial and cybercriminal activities, including cash-out schemes. Therefore, an analysis of around four million Dutch Telegram messages from 2017 to 2021 was conducted, which revealed a discrepancy between the actual usage of payment methods and the patterns suggested in existing academic literature. Notably, Bitcoin ranked fourth among the payment options utilised, following Paysafecard, PayPal, and Tikkie. Furthermore, it was observed that privacy coins were not requested by vendors in their advertisements.

2.2 Research Gaps in Current Literature and Practice

Much (quantitative) research into cybercrime communities has already been undertaken. However, the amount of research into Telegram communities is relatively limited and significant gaps remain in understanding the full scope of these communities, particularly regarding the rapid evolvement of *modi operandi* in criminal environments and the mechanism in the Telegram ecosystem driving these evolvements on community level.

Mechanisms behind Change of Criminal Modi Operandi

Research on underground cybercrime communities has recognised the role of systemic mechanisms, such as platform regulations, technological advancements, law enforcement interventions and trust-building, in sustaining illicit markets. However, in the case of Telegram-based criminal ecosystems, these structural enablers remain poorly understood. While it is evident that modi operandi evolve rapidly, the underlying community-level mechanisms driving these changes are largely unexplored. Research has yet to identify which factors make enforcement difficult, how illicit actors mitigate the risks of takedowns (for example through security measures), and why Telegram as an illicit market continues to thrive despite heightened moderation efforts. Besides, it is unknown how commoditisation and automation shape the exchange of goods and services within Telegram.

Rapid Shifts of Modi Operandi

Furthermore, quantitative research on underground communities have often been performed on outdated data, risking not only generalisation errors but also limiting the ability to accurately reflect current trends in rapidly evolving underground communities, leaving critical knowledge gaps (Boekhout et al., 2024). Longitudinal approach particularly often relies on the availability of existing data, as a commonly shared challenge is the lack of available data (Hughes et al., 2024). Three aspects play a vital role in the limited availability of data that can be used, namely (I) the increased use of message encryption in communication, (II) the use of jargon, and (III) the fact that various platforms are invite-only, proposing challenges to enter communities (Boekhout et al., 2024; Hou et al., 2022; Hughes et al., 2024). The use of potentially outdated data can result in findings that do not accurately reflect recent trends, especially given the rapidly evolving nature of underground communities. Consequently, much research depends on previously collected data, with only 55% of studies utilising self-scraped data (Hughes et al., 2024).

These rapidly evolving behaviours are for example evident in payment preferences, where underground markets have seen significant shifts. While virtual currencies, such as Bitcoin, were traditionally the primary means of payment; '*Bitcoin is unquestionably the preferred digital currency in the Darknet,...*', newer forms of transactions have gained usage in recent years (Demant et al., 2018; Kuzuno & Tziakouris, 2018, p. 2644). Today, alternative payment methods such as Paysafecard, PayPal, and mobile payment platforms like 'Tikkie' are increasingly common (Schrama et al., 2022). The same rapid shift can be seen in modi operandi (Baraz & Montasari, 2023, p. 68). As a result, even research that appears recent can quickly become outdated as these markets continue to innovate, underscoring the need for continuous data collection to capture these dynamic shifts.

The absence of up-to-date and self-retrieved data limits the ability to identify how modi operandi are directly influenced by interactions between criminal actors and ecosystemic mechanisms. Without addressing this gap, law enforcement agencies and policymakers lack the necessary tools to design effective, tailored interventions on current trends.

Missing Community-Centric Cybercrime View

Most cybercrime measurement studies focus on specific crimes, such as malware, drugs, or money laundering, rather than examining the broader cybercrime ecosystem (Van Wegberg et al., 2020). This fragmented approach overlooks how modi operandi (offerings of illicit products, services, payment methods and the way in which this is offered) interact with (alterations in) the ecosystem, limiting understanding of market dynamics and adaptability. A community-centric view is often missing, yet crucial, as underground markets operate as interconnected ecosystems where shifts in one area influence others. Large-scale analyses, with self-retrieved data, have demonstrated the value of studying these networks holistically, providing deeper insights into their resilience and evolution of communities, key for more effective enforcement strategies (Roy et al., 2024; Schrama et al., 2022). By contrast, it is yet unknown how specialisation of communities contributes to the overall resilience of Telegram as a market. This can provide greater insight into the question of whether the dismantling of (parts of) communities results in a reduction of exhibited crime.

3 Research Design and Methodology

Based on the found knowledge gaps in the state-of-the-art, Chapter 3.1 elaborates on the research's primary aim and defines the scope and approach. Chapter 3.2 outlines the central research question and supporting sub-questions that guide the study. It explains how each question contributes to understanding the relationship between system evolutions and behavioural adaptations in cybercrime communities. In Chapter 0, the mixed-method approach used in this study is explained, outlining the rationale for the chosen methods, the purpose of their implementation, the high-level criteria for optimal model performance, and the dataset utilised for these analyses. The quantitative research process involves making numerous modelling decisions regarding the research design; therefore, Chapter 6 (Detailed Quantitative Approach) is added to elaborate in detail on the undertaken steps.

3.1 Research Objective

The objective of this research is to improve the understanding of the systemic mechanisms driving adaptive cybercrime behaviours. The impact of platform regulations, technological advancements and law enforcement interventions on the behaviours and operational methods (*modi operandi*) is yet unknown, therefore, this research aims to close the existing proposed gaps. This study therefore seeks to link the mechanisms driving these dynamic adaptations and their broader implications for the cybercrime ecosystem, measured as actual exhibited behaviour by Telegram users using operational, technical, financial, and behavioural perspectives. Telegram, as a widely utilised and accessible platform in the Dutch criminal ecosystem, serves as a case study to examine these phenomena. The platform's user-friendliness, having the (former) image of performing minimal regulation, and thereby enabling criminal activity, offers a lens for exploring both the drivers of criminal behaviour and potential enforcement opportunities.

By analysing both quantitative behavioural data from Telegram communities and qualitative theoretical frameworks, this study first seeks to identify the structural enablers of cybercrime adaptation and resilience in the Telegram ecosystem. Specifically, it aims to examine how users and administrators exploit platform functionalities to structure, scale and sustain their operations. Additionally, the study explores channel continuity, the mechanisms that enable illicit markets to persist despite enforcement and moderation efforts. This can determine whether efforts lead to meaningful disruption, solely result in crime displacement, or that crime is continued in other ways. Finally, it investigates the specialisation and professionalisation of vendors, assessing how product diversification, payment preferences, and operational expertise contribute to the resilience and interconnectedness of Telegram as an illicit ecosystem. In doing so, this research enables law enforcement agencies to develop more targeted and effective interventions by aligning empirical data with law enforcement strategies. Furthermore, by developing a reproducible methodology and using public communities, this study not only contributes to the immediate understanding of Dutch cybercrime dynamics but also provides a scalable framework to use this research as a base case. The results of this study are intended to improve the effectiveness of enforcement initiatives, guide policy development, and serve as a benchmark for understanding the broader evolution of cybercrime ecosystems in a changing digital landscape.

Given the limited scientific research on behaviour and trends within Telegram marketplaces, it is essential to contextualise the quantitative findings. This is achieved in part by using theoretical concepts as a lens to interpret empirical data. Additionally, comparisons with previous Telegram trends are facilitated by building on an earlier study and its dataset on Dutch Telegram groups by Schrama et al. (2022) as a reference framework. The results from that study serve as a benchmark, enabling this research to generate new insights and expand upon previous findings in comparing community behaviours. Rather than replicating the study, this research uses their insights as a foundation for understanding broader trends. However, since this study employs partially different analyses and methodologies, it is occasionally necessary to consult the dataset which served as the foundation for that study and replicate parts of certain analyses, to enable effective comparison of trends over time. While the underlying data, messages from Dutch Telegram groups, shares similar characteristics, this study adopts a broader perspective on the criminal Telegram ecosystem than the reference study, which primarily centred on cybercrime, financial crime, and the role of virtual currencies.

3.2 Research Questions

Following the research gaps and the objective, the following Research Question has emerged:

RQ: What ecosystemic mechanisms stimulate the resilience of Telegram as an illicit market?

To be able to answer the research question, a mixed-method approach is utilised. Thereby, both qualitative and quantitative methods are used interchangeably. First, exploratory research and establishing a theoretical fundament are necessary to understand the concepts that are frequently drawn upon and to be able to provide a theoretic lens to guide the results of the (quantitative) part. Therefore, sub-question I is defined as:

- SQ I: *Which mechanisms enabling behavioural adaptation are observed by law enforcement agencies and in literature?*

The first phase focuses on exploring ecosystemic mechanisms from theoretical and law enforcement perspectives. This is essential to develop a framework that contextualises the quantitative findings and guides the interpretation of empirical patterns. The second phase transitions into a quantitative analysis, using independently collected (Dutch) Telegram data. The goal is to empirically assess how actors operate, maintain, and adapt illicit activities on Telegram, building on the theoretical insights from the first phase. The following sub-questions guide this phase:

- SQ II: *How do users and channel administrators exploit technological capabilities to structure and operate illicit Telegram channels?*
- SQ III: *What mechanisms facilitate the continuity of Telegram as an illicit market?*
- SQ IV: *How does specialisation by channels and individuals contribute to the adaptability of Telegram as an illicit market?*

With these sub-questions, first, it investigates the technological capabilities used by users and administrators to sustain illicit channels, such as automation, self-regulation, and moderation tools. Second, it examines the factors that contribute to channel continuity, and how illicit markets persist through adaptation, migration, and enforcement evasion. Last, it explores the specialisation of vendors and channels, analysing how differences in product offerings, specialisation, professionalisation, and market dynamics shape the ecosystem's resilience. Together, these sub-questions provide a multi-layered perspective on how Telegram's criminal ecosystem evolves.

3.3 Methodology

By relying solely on a qualitative or quantitative lens, it becomes difficult to contextualise empirical findings or link them to previously explored phenomena in the literature. A mixed-methods approach enables the integration of findings, allowing empirical data to be interpreted within a broader framework of existing research (Creswell, 2009). This way, identified phenomena can guide results and help interpret trends in their contexts. This chapter will explain the rationale behind the used methodology per phase (qualitative and quantitative), as well as present the necessary underlying data and the criteria that this must meet.

3.3.1 Rationale for Qualitative Analyses

Objective:

Desk research and interviews are used, which serve a dual purpose. First, they aim to identify the system characteristics and concepts most frequently discussed in the literature on illicit marketplaces. These theoretical insights will provide a framework for interpreting the findings from subsequent quantitative analyses. As the availability of literature on Telegram behaviour is relatively limited, parallels must be drawn with characteristics of

longer-established communities. Defining and conceptualising potential behaviours is critical for establishing, to a certain degree, measurable indicators that can be applied in further stages of this research. While Chapter 2 has briefly mentioned some of these system characteristics, this phase seeks to enable drawing deeper parallels between the empirical findings and existing literature after performing the quantitative analyses. Using theoretical lenses to interpret the data ensures that observed trends are contextualised within established academic concepts. The literature review thus serves as a tool to identify expectations that may arise in the current Telegram dataset and to align these with observed empirical trends.

Although this study has acknowledged the limitations of prior research, it uses a literature review not as a definitive source but as a lens through which to validate and contextualise empirical findings. This approach, beginning with a broad exploration of system characteristics and narrowing down to understand specific factors, ensures a robust foundation for quantitative analyses. By integrating qualitative insights with empirical data, the mixed-methods approach adopted here improves both the depth and validity of the research, enabling a better understanding of how criminal ecosystems adapt and evolve.

Second, the theoretical concepts are contextualised by aligning them with the insights gained from expert interviews, thereby bridging the gap between theoretical frameworks and real-world observations from Dutch (cyber)crime environments. The expert viewpoints complement one another, offering diverse perspectives on enforcement challenges, criminal adaptation, and market resilience. However, given that each expert specialises in a different area of cybercrime investigation, these insights should be viewed as illustrative rather than universally representative or exhaustive and can therefore be presented in a coherent narrative. Aligning empirical findings with expert insights and literature is essential for several reasons. First, expert opinions and theoretical frameworks provide a baseline against which scraped marketplace data can be compared. This comparison allows for the identification of key system characteristics and behavioural patterns that influence participant actions. The literature review and interviews are expected to uncover additional elements, besides the identified systemic factors identified in Chapter 2.1.2, that may have significant implications for online criminal behaviour and its interpretation.

Method:

The literature review aimed to address gaps in understanding criminal behaviour on Telegram by drawing insights from research on dark web marketplaces and forums. Using Google Scholar and Scopus, supplemented by the snowballing method, relevant sources were identified and analysed. Previously reviewed literature was also revisited for alignment with the study's objectives. The following query was used for the first step:

('criminal behaviour' OR 'criminal activity' OR 'cybercrime') AND ('telegram' OR 'dark web' OR 'darknet' OR 'underground markets' OR 'online forums') AND ('shifts' OR 'adaptation' OR 'evolution' OR 'trends' OR 'changes') AND ('law enforcement' OR 'intervention' OR 'modi operandi')

As Telegram remains underexplored compared to dark web platforms, literature on these forums provided a comparative foundation for understanding influencing factors and their relevance to semi-public channels. This inductive approach, similar to that of Aldridge and Decary-Hetu (2015), and Soska and Christin (2015), places Telegram's dynamics within broader trends observed in other criminal ecosystems.

The second component of the qualitative research consists of semi-structured interviews. The interviews involve Dutch experts from various investigative agencies, knowledge institutions and/or law enforcement. Data saturation is achieved when a broad understanding of the prevailing trends, the adaptive behaviours of criminals, and the responses of the relevant agencies to these evolving trends is established. Additionally, it is essential to consider whether conducting more interviews will yield new insights or if it will merely consume valuable time throughout the entire process. For this reason, it is initially assumed that three to five interviews will be conducted until data saturation is achieved. The interviews focus on three key themes to understand trends and aim to place the earlier-found concepts into perspective. The complete interview protocol is presented in Appendix A. The first theme

examines crime types and strategies, exploring how criminal tactics have evolved over the past years, and trying to capture any observable shifts in criminal strategies from the perspective of law enforcement agencies. The second theme investigates payment methods, assessing shifts in preferences and whether there has been any noticeable change in these methods. The relationship between payment methods and criminal tactics is also examined. The third theme explores community behaviour, focusing on how networks adapt to system changes, such as law enforcement interventions or technological innovations. The role of anonymity in these adaptations, particularly on platforms like Telegram, is also examined.

During all interviews, notes were taken, and the key themes and trends were documented. When recording the interview was permitted, these recordings were transcribed using a locally installed version of the open-source artificial intelligence software Whisper, developed by OpenAI. This programme has demonstrated a low word error rate in recognising speech in both Dutch and English (Radford et al., 2022). Subsequently, the transcriptions underwent a manual review to identify and correct errors in misunderstood words and sentence structures without improving verbatim language issues, such as speaking errors, stuttering, or repetitions, as addressing these would significantly increase the workload while contributing minimally (Eaton et al., 2019). A summary highlighting key points and trends from all interviews was compiled and integrated into a context study, presented in Chapter 5. The identities of the respondents and corresponding organisations remain confidential throughout this study. Instead, references will be made to the role of the respondent, and the findings from the interviews will be incorporated into a global summary of all interviews conducted. The recordings of the interviews were deleted after transcription.

3.3.2 Rationale for Quantitative Analyses

Objective:

The quantitative approach serves several specific purposes. First, by analysing technical, structural, operational, and financial aspects, this research seeks to understand how illicit Telegram channels adjust to enforcement measures and platform regulations. Through this, it becomes possible to identify the mechanisms driving concrete behavioural shifts, *modi operandi*, and emerging trends, particularly by drawing longitudinal comparisons with the reference dataset. This historical perspective allows for a deeper understanding of how Telegram's illicit ecosystem evolves over time. Second, beyond tracking mechanisms enabling adaptation, this research aims to dissect the internal structure of illicit Telegram communities, exploring vendor specialisation, professionalisation, and payment preferences. Understanding the organisational dynamics of these marketplaces is critical to determining how Telegram facilitates illicit activity and whether vendor or channel specialisation contributes to resilience. Examining how vendors operate, the extent to which they diversify their offerings, and their payment strategies will provide insights into the economic and structural sustainability of these criminal networks. Third, recent insights from data are bridged with theory. While conceptual frameworks such as crime displacement, commoditisation, and illicit market resilience offer valuable perspectives, they are often difficult to quantify directly. By systematically analysing behavioural patterns and trends, this study aims to provide empirical grounding for these theoretical constructs. This approach ensures that the findings are not just descriptive but also contribute to broader criminological and cybercrime research. Last, the methodology of this study is designed to be reproducible and comparable, allowing for future longitudinal analyses. By establishing a structured approach to measuring Telegram's illicit market, this research can serve as a foundation for ongoing studies into criminal adaptability, platform regulation impacts, and evolving cybercrime strategies. The results of this study not only provide immediate insights into Dutch Telegram communities but also contribute to the long-term development of data-driven cybercrime research.

Data:

The accessibility of Telegram, requiring minimal technical expertise or additional resources, is evident in both Dutch and international communities, where criminal goods and services are openly traded, often with surprising transparency. Also, Telegram messages can offer a wide array of information. Communication within illicit Telegram channels can be categorised into four main types of messages: offer and request advertisements, chat messages, and bot messages. This provides information regarding the exchanged goods and services but also offers insights into the topics discussed by criminals and the types of bots employed by administrators. This, in turn, indicates the

level of professionalism and organisation present within trading channels. Furthermore, the platform enables researchers to observe activities passively, which is often referred to in the literature as *lurking* or *cyber stealth* (Roks & Monshouwer, 2020). This allows to gather insights without directly engaging with the community, thus minimising ethical concerns and avoiding disruptions to natural behaviours. Telegram's API improves its suitability by allowing the efficient extraction (scraping) of complete chat histories with relative ease. Although this process can be time-consuming and presents certain challenges, it allows for the downloading and analysis of substantive chat messages for further research.

The decision to focus exclusively on Telegram is strategic. Introducing multiple platforms into the analysis could skew the results by introducing platform-specific effects, complicating efforts to identify broader trends. Telegram's prominence in facilitating criminal activity, combined with its accessibility and the depth of data that it can offer, ensures that this platform serves as a proper and focused lens through which the evolving dynamics of criminal behaviour in digital marketplaces can be studied.

The data from Telegram is independently sourced, rather than using an existing dataset. First, self-scraped data ensures control over the quality, scope, and relevance of the dataset. Existing datasets can come with limitations, such as outdated information, predefined structures, or missing metadata, which may not align with the specific research questions. Scraping the data directly allows for a tailored approach, capturing precisely the type of messages, timeframes, and criminal categories relevant to the study. Moreover, relying on external datasets introduces potential biases, as the context and methods of data collection might not be fully transparent or are misaligned with the current scope. Furthermore, independent scraping ensures transparency and reproducibility in the research process, as the methods and parameters can be documented and verified. Lastly, Telegram's rapidly evolving landscape requires up-to-date data to accurately reflect current trends and dynamics. Pre-existing datasets may lack this timeliness, making them less useful for identifying recent developments in criminal behaviour.

The exact number of channels and messages that need to be scraped is not determinable upfront but is influenced by a few aspects. Important patterns need to be identified while ensuring that data captures the diversity and complexity of criminal activity on Telegram. A larger dataset improves the robustness of findings, particularly when examining nuanced behaviours or rare categories, and behavioural patterns. Besides, the dataset should ideally span messages from a sufficient timeframe to enable the identification of long-term trends. A narrow window of observation might capture short-term fluctuations but could fail to reveal deeper shifts in behaviour. Although trends and results can be identified by building on the reference dataset, the concentration of messages within a short timeframe may obscure shifts in current behaviour. Furthermore, certain trends, such as crime displacement, may take months to develop and require longitudinal data to capture effectively. Extending the dataset across multiple years allows this research to place findings within a broader temporal context, providing a more nuanced understanding of how criminal activities evolve and adapt over time.

The Telegram channels included in this study were selected based on specific criteria designed to ensure that the identified channels fulfil the set criteria for this research and that the channels truly represent the Dutch (cyber)crime landscape. (I) Channels were required to predominantly use Dutch, as indicated by their titles and internal communication. This focus ensures the study's relevance to Dutch law enforcement. However, Flemish-language channels were also included, as the linguistic and geographic overlap between the Netherlands and Belgium facilitates a shared trade network, particularly in border regions, making it difficult to exclude such channels without losing critical data. (II) To prevent redundancy with previous research conducted on Dutch Telegram marketplaces, the messages examined in this research were restricted to those after February 2021, through November 2024. Although changes observed solely within this timeframe may not be definitive, being able to compare it to the reference dataset allows for a comparative analysis of criminal behaviour and operational methods, building on the findings of earlier studies and identifying potential shifts over time. (III) Only public Telegram channels were included in the analysis, as they are accessible, reduce ethical concerns and ensure that the collected data is replicable. Private channels, often restricted by invitation-only access, pose significant challenges in terms of both accessibility

and ethics, and the behaviour witnessed in closed channels cannot be compared to that observed in open channels. (IV) Last, channels had to display evidence of illegal trade and had to offer all current and emerging crime types to be able to reach data saturation. This includes channels that might appear legitimate, such as car marketplaces, but contain a significant volume of illegal advertisements. This approach ensures that the full spectrum of criminal activities is captured, including illicit trade in seemingly lawful contexts (e.g. car trade channels).

At the time of writing, Telegram appears to be undergoing a potential shift in its role as a platform for criminal activities. Recent announcements indicate that Telegram may begin sharing phone numbers and IP addresses with authorities, which could significantly impact data availability and alter criminal *modi operandi*, which could drive criminals toward alternative communication platforms. The implications of this shift could be twofold. On the one hand, this external pressure presents an excellent opportunity to observe how criminal networks adapt to changes in their operating environment, potentially yielding valuable insights into the resilience and adaptability of these communities. On the other hand, such changes could result in reduced data availability on Telegram, as some channels may migrate to other platforms, making it more challenging to capture a picture of criminal behaviour on Telegram. This latter scenario may particularly affect activities involving serious crimes, such as arms trafficking and child pornography, as these are more likely to be the focus of law enforcement data requests.

This research acknowledges the ethical concerns associated with analysing large-scale personal message data. To mitigate privacy risks, only publicly accessible Telegram channels were scraped, ensuring that no private conversations or restricted content were included. Telegram's privacy policy explicitly states that messages shared in public channels are considered public information, which users consent to upon account creation (Telegram, n.d.-b). Therefore, the use of this data aligns with ethical research practices. Additionally, strict measures were implemented to minimise data collection, capturing only essential metadata such as channel names, anonymised Author IDs, timestamps, message views, shares, and content. The Author ID is an alphanumeric string that does not reveal usernames or aliases, preventing any conclusions from being linked to individuals. Furthermore, to maintain confidentiality, the names of the analysed Telegram channels will not be disclosed in this study. Last, no responses or advertisements are solicited, as the author of this research has not sent any messages. This ensures that no forms of *'honeypotting'* are exhibited.

Method - Scraping

To achieve the objectives set for the quantitative analyses, four key steps methods are employed. This chapter outlines the rationale behind these chosen methodologies, providing insight into why these approaches are suitable for addressing the research questions. This section focuses on the overarching principles guiding the quantitative work. The detailed design choices made during the execution of each method and an overview of the quantitative methods (through a research process flowchart) are explained in Chapter 6.

The methodology for data scraping is designed to ensure that the dataset collected accurately reflects the Dutch criminal ecosystem on Telegram. Therefore, the process begins with the manual identification of Telegram channels. Automation cannot reliably filter channels based on set criteria such as language, activity level, and relevance to criminal activities. By manually assessing potential channels against these criteria, the research ensures that the dataset is complete and specifically aligned with the scope of the study. This manual intervention helps to avoid irrelevant data and focuses on channels that provide the most valuable insights into the Dutch criminal landscape. Data collection is conducted using an improved open-source scraper modified to optimise the efficiency of the scraping process and usability of data. Rate-limiting is used to mitigate risks of detection by Telegram. Further preprocessing steps are used to reduce noise in the dataset and to optimise the data for further usability. The scraping process ultimately yielded 1,389,624 (non-empty) messages, originating from 14,856 unique users in 45 identified Telegram Channels, which fulfilled all the set criteria. All messages were sent between 20-02-2021 and 20-11-2024. Chapter 6.1 elaborates on the detailed used scraping techniques.

Method - Classifying

The scraped data provides valuable insights into general trends within the channels, such as the number of messages sent and the number of subscribers per channel. Furthermore, this data can serve as a foundation for more in-depth analyses, including the categorisation of crime types, payment methods, and conversation topics. To enable these analyses, it is crucial to determine with a high degree of certainty the subject of each message. Accurately classifying message types and crime categories is essential for this reason. Manual labelling all messages is time-intensive, therefore, a machine learning model has been used. Among the three main types of machine learning (unsupervised, supervised, and reinforcement learning), supervised learning is the most suitable for this task. Unsupervised learning clusters data without labels, which is useful for uncovering hidden patterns but insufficient for producing precise class labels like 'Ad. - Offer' or 'Chat Message' (Alloghani et al., 2020, p. 4). Reinforcement learning is effective for decision-making tasks, but less practical for text classification due to its reliance on iterative rewards and complex interactions (Kober et al., 2013). Supervised learning, however, uses manually labelled data to train models that recognise patterns for accurate new predictions, making it ideal for categorising Telegram messages. Support Vector Machines (SVM) are particularly effective for text classification due to their ability to handle high-dimensional, sparse data (Aggarwal & Zhai, 2012; Sebastiani, 2002). Unlike regression models, which predict continuous values, SVM specialises in classification tasks, achieving high performance on binary tasks even with limited datasets. By utilising a hyperplane to separate classes, SVM ensures efficient and accurate classification, which is critical for analysing Telegram messages with high accuracy. Supervised classification models include Logistic Regression, Random Forests, Naive Bayes, and deep learning methods like Neural Networks. Among these, Support Vector Machines (SVM) excel for text classification tasks due to their ability to handle high-dimensional data efficiently (Pranckevičius & Marcinkevičius, 2017).

To train the SVM model and to be able to develop a predictive model capable of accurately classifying messages by message type and ad category, it is essential to have (manually) labelled messages. There are two primary methods to obtain these messages. Firstly, one can label the messages manually, a process that is time-consuming but ensures that the labels applied are highly relevant to the new data. Alternatively, it is possible to reuse pre-labelled messages from existing datasets. However, this is contingent upon the data and labels meeting specific criteria. Ensuring high quality of the labelled data and thus that the messages are labelled as accurately as possible is crucial for guaranteeing the validity and reliability of subsequent research methods. This study adopts a hybrid approach, utilising both newly independently labelled messages and those that are readily available, originating from research by Schrama et al. (2022). This decision was driven by the advantages offered by combining the two datasets, making a balance between using the strengths of existing resources and addressing their limitations. Solely relying on pre-existing data would have limited the scope and specificity of the labels to the original research context, potentially leaving gaps in the classification of emerging crime types or behavioural patterns not previously captured. Alternatively, independently labelling the entire dataset would have been time-intensive, especially given the luxury of having access to a substantial amount of pre-existing labelled data. Furthermore, during the manual labelling process, challenges were encountered, such as the use of slang or messages only containing pictures and/or videos (which were not captured during the scraping process), which ultimately complicated the labelling process and inherently resulted in unwanted labelling errors, which has been estimated in Chapter 6.2. By using a hybrid approach, the reliability and prediction power of the model could be further improved.

For the manual sampling, stratified sampling was chosen over other techniques like random sampling to ensure a good representation of all Telegram channels in the labelled dataset. By treating each channel as a distinct stratum, this method guarantees that every subgroup contributes proportionally to the sample, preventing the overrepresentation of dominant channels or the underrepresentation of smaller ones (Meng, 2013). A percentage of messages from each channel will be labelled, adhering to defined upper and lower limits, alongside incorporating previously labelled data to create a balanced and representative dataset. This reuse of pre-existing labels is justified for several reasons. The nature and origin of the messages remain consistent, with overlapping channels and only the scraping period differing, which poses no challenges. The integration of old labels is feasible by aligning their distributions with the current dataset, ensuring they don't disproportionately influence the training model. This

balance will be tested for necessity. Expanding the training dataset improves the SVM model's generalizability, reducing overfitting and improving accuracy for unseen messages (Uma & Rathiga, 2024). Last, the use of previous labels is feasible due to their consistency and uniform application. To achieve this, the previously labelled data was thoroughly examined, and new messages were labelled with the same annotation methodology, reducing the risk of introducing bias or discrepancies that could arise from entirely new labelling efforts.

The number for the labelled dataset size in this study (including manually labelled messages and reused labels) is not fixed. The primary objective is to ensure the model can accurately predict labels for new messages. In the reference study, 0.5% of the dataset was labelled, showing a balance between labelling effort and model performance. While 0.5% proved effective, increasing the proportion of labelled messages often improves model training, particularly for complex datasets where message content varies widely or where some categories have low representation. Categories with fewer training examples are more prone to misclassification during the training process, especially as not all data is used for training (but also for testing and optimising the model). By increasing the size of the labelled dataset, the models can better learn the nuances of the data, reducing the likelihood of overfitting and improving their ability to classify unseen messages accurately. Ultimately, 0.2% of the current dataset was manually labelled (3,873 messages). This was supplemented with the full set of previously labelled data from the reference study, exceeding the 0.5% threshold in doing so.

To identify the best-performing model configurations, several iterations were conducted, varying input parameters while keeping all other variables constant (*ceteris paribus*). The model's performance was assessed using precision and recall, which measure the accuracy of predictions and the ability to identify all relevant instances, respectively. These metrics ensured that the models were not only accurate but also effective in capturing diverse message types and categories. Certain message categories posed challenges due to their low absolute representation in the dataset. This was addressed by incorporating the full pre-existing labelled dataset, which provided additional training examples for underrepresented categories. For the message type classification model, further balancing techniques were used to ensure that the minority classes received sufficient attention during training. Given the important role of message type classification in the overall analysis, the message type model was prioritised in cases where trade-offs between the two models were necessary. Accurate categorisation of advertisements, chat messages, and bot messages forms the basis for all subsequent analyses. While precise categorisation of advertisement types is important for understanding the relation between crime types and payment methods, other analyses are impacted minimally by misclassification. Further technical details, including the detailed labelling methodology, the coding approach, and the steps taken to optimise the model, are provided in Chapter 6.2.

Method – Topic Modelling

Third, to systematically analyse and summarise the high volume of chat and bot messages, topic modelling using unsupervised machine learning is performed. Unlike supervised methods, which require predefined outputs, unsupervised techniques like *Latent Dirichlet Allocation* (LDA) autonomously identify patterns and themes within unstructured data, making them ideal for highly variable and unpredictable text content (Hughes et al., 2024; Porter, 2018). LDA assumes that each document (or message) can relate to multiple topics, which allows for categorisation (Blei et al., 2003; Hughes et al., 2020). The model identifies latent topics by analysing the distribution of terms within the data, with each topic defined by a weighted combination of words (Blei et al., 2003). This process assigns a topic distribution to each document, revealing the prominence of various topics within it. By examining these distributions across all documents, the analysis uncovers the key themes discussed in the chat messages within the Telegram channels. As topic models are performed unsupervised, the results must be manually validated to ensure that meaningful topics emerge, including the selection of the appropriate number of topics and hypertuning certain parameters if necessary. Validation also includes using domain knowledge to assess the relevance of words in each topic and reviewing sample texts associated with each topic.

The LDA model was conducted twice on the current dataset to analyse chat messages and bot messages separately. By treating these as distinct datasets, the analysis aimed to uncover differences in the themes present

in direct human interactions versus automated bot communications. This separation allows for a better understanding of how criminals use Telegram, particularly as bot messages often serve functional or administrative roles, while chat messages are used for broader discussions. The expectation was that these models might reveal different latent topics, with chat messages highlighting criminal interactions and bot messages offering insights into channel management or operational practices. The results of the LDA on the current dataset provide insights into the topics currently discussed within the channels. However, to determine whether these topics have shifted over time, it is necessary to perform the LDA analysis on the chat messages from the reference dataset as well. This dual-dataset approach will help identify potential changes in themes and trends, helping identify shifts in criminal priorities, emerging trends, or external influences such as law enforcement interventions or technological changes.

Method – Automated Indexing

The final stage of the quantitative analysis examines the link between crime types and specified payment methods in advertisements, aiming to uncover patterns in the operational choices of criminals. By analysing how payment methods vary across crime categories, this research seeks to understand the financial tools criminals use. Besides, payment methods often reflect the nature and scale of transactions, and when comparing the number of accepted payment methods with the number of offered crime types, more insights about the differences in *modi operandi* between single-category and multi-category vendors can be derived. Understanding these preferences offers intelligence for law enforcement and policymakers by highlighting vulnerabilities in (legitimate) financial systems that criminals exploit. Moreover, tracking shifts in payment methods over time reveals broader behavioural trends, potentially showing changes in trust, regulation, or criminal strategies. Unravelling these patterns was done via an approach similar to that of Schrama et al. (2022), which has proven to be effective and relatively easy to implement. This begins with systematically filtering advertisements offering goods or services. After locating signal words and looking around these words for predefined keywords indicating payment methods, the found payment methods can be linked to their (already known) label for the advertisement category, enabling the possibility of making connections between these variables. Manual inspections have redefined the lists with payment indicators to ensure accuracy and to address false positives, such as terms like 'crypto' or 'tikkie' being used in a different context (rather than as payment methods).

4 A Theoretical Lens on Adaptation and Resilience in Illicit Markets

The literature presented in this chapter is intended to provide context and foundational knowledge rather than to directly compare or contrast different scholarly perspectives. Its primary purpose is to gather insights from existing research, offering an understanding of the systemic characteristics and dynamics of illicit online marketplaces. This theoretical foundation serves as a guiding framework for the quantitative analysis conducted in later stages of this study. By aligning empirical findings with established concepts from the literature, this approach enables a more nuanced interpretation of observed patterns, ensuring that quantitative insights are contextualised within broader academic literature. Literature has been identified following the methodology outlined in Chapter 3.3.1.

Existing research has mainly examined underground forums and marketplaces on the dark web, with less focus on Telegram channels, likely due to the relatively recent emergence of this communication medium by criminals. Consequently, this review incorporates literature on dark web marketplaces and forums for comparative purposes. Understanding the factors influencing underground channels is crucial, as these factors may similarly impact semi-public channels. Popular scholars in this field, such as Aldridge and Decary-Hetu (2015), and Soska and Christin (2015), have used this same method to get a better understanding of drug trafficking in general, by exploring virtual drug markets. The same inductive approach is used to understand Telegram channels by exploring the symptoms and implications of changing system environments of other criminal communication methods.

4.1 Exploring the System Environment

4.1.1 Law Enforcement

Understanding the strategies employed by law enforcement agencies (LEAs) to counteract cybercrime is critical for analysing how criminal networks adapt and respond to external pressures. Despite various interventions, the resilience and adaptability of these networks challenge the long-term efficacy of traditional approaches (Ladegaard, 2020). Evolving criminal ecosystems often outpace conventional investigative methods, necessitating innovative and adaptive law enforcement strategies (Devlin et al., 2024).

Two broad categories of LEA interventions are identified: infrastructural policing and influencing tactics. Infrastructural policing targets the technological and operational foundations of cybercrime networks, such as disabling key components or apprehending facilitators, which often results in short-term disruption but rarely leads to permanent solutions (Collier et al., 2022; Van Buskirk et al., 2017). Influencing tactics, on the other hand, aims to alter offender behaviour through deterrence, particularly among less experienced offenders. However, seasoned cybercriminals often remain unaffected and continue to evolve their practices (Collier et al., 2022).

A comprehensive framework for law enforcement actions distinguishes four primary functions: reactive, incapacitative/deterrent, disruptive, and preventive measures (Collier et al., 2022). Reactive measures respond to specific reported incidents, often working alongside communication and/or social platforms for content moderation. Incapacitative and deterrent actions focus on high-profile arrests of key actors to discourage broader participation in cybercrime, as seen in recent Dutch operations targeting data traders facilitating other crimes (Politie, 2024). In the same operation, users of illegal channels have been alerted through a warning message, aiming to achieve a deterrence effect and to raise awareness regarding potential consequences. Disruptive efforts, often supported by private actors, aim to destabilise infrastructure by dismantling botnets or removing illicit platforms. Last, preventive strategies target both victims and potential offenders, raising public awareness to reduce vulnerabilities while using digital tools, like targeted ad campaigns, to deter criminal behaviour.

However, in doing so, law enforcement agencies face various types of challenges, which hinder the efficacy of the performed actions and the ability to carry out new interventions. These challenges, actively exploited by criminals

to evade detection, include technological aspects, jurisdictional complexities, criminal adaptability, resource constraints, and limited public-private collaboration. Understanding these challenges is critical to examine how they shape offender behaviour on platforms like Telegram and how they influence the broader dynamics of cybercrime. Although not all these systemic issues are directly observable within this study, their implications provide important context for analysing Telegram's role in facilitating criminal activity. First, technological innovation poses significant obstacles, as new tools improve anonymity and obscure criminal activities, outpacing the capacity of traditional forensic and legal systems (Amoo et al., 2024; Baraz & Montasari, 2023). Telegram, widely perceived as secure, lack full encryption for default channel and chat interactions, making them less private than alternatives like Signal. However, criminals exploit Telegram's minimal regulatory oversight for illicit activity. Second, jurisdictional challenges further complicate enforcement, as the cross-border nature of cybercrime involves global networks and supply chains. Effective international collaboration is often limited by sovereignty concerns and privacy regulations, which restrict evidence collection (Amoo et al., 2024; Baraz & Montasari, 2023; Warner, 2023). While this study focuses on Dutch Telegram channels to maintain jurisdictional relevance, potential links to international networks remain a relevant but secondary consideration. Third, criminals' adaptability is a significant challenge, as they respond to enforcement actions in different ways (relocation, fragmentation or increasing security). This persistent 'cat-and-mouse' dynamic highlights how interventions drive criminal innovation (Baraz & Montasari, 2023; Soska & Christin, 2015). Telegram's perceived security has made it popular among criminals, but recent announcements about sharing user data with authorities could lead to behavioural shifts (Krikhaar, 2024; Wokke, 2024). At the moment of writing, the precise results of the data exchange between Telegram and law enforcement agencies remain unclear. Research will determine whether these increased concerns are also shared among Telegram users. Fourth, resource constraints pose another significant barrier. Cybercrime investigations are resource-intensive, often limited by insufficient budgets, outdated tools, and staffing challenges. These limitations force law enforcement to prioritise severe forms of criminal activity, potentially driving offenders to adapt their methods or shift focus to less-policed areas (Devlin et al., 2024; Kuzuno & Tziakouris, 2018). Finally, the lack of collaboration between law enforcement and private sector actors limits the effectiveness of interventions, as the limited partnerships prevent law enforcement from leveraging the advanced technological capabilities of private companies effectively, leaving enforcement efforts lagging behind innovation (Amoo et al., 2024; Baraz & Montasari, 2023).

Users of these markets respond in two ways, with a clear distinction between oblivious and cautious users, in reaction to performed or announced interventions (Ladegaard, 2018). First, oblivious users are unaware of (new) threats and keep performing their activities, as long as marketplaces, forums or payment methods keep operating. Cautious users develop caution and modify their actions in reaction to perceived threats on the other hand. These types of paranoia about infiltration by law enforcement are often recognised among users of darknet marketplaces and illicit Telegram channels. This leads to behaviour such as closing membership temporarily or adopting stricter vetting processes during high-risk periods, such as major political events (Mador, 2021). Additionally, there is a low level of awareness about how law enforcement operates, which sometimes works to law enforcement's advantage but can also be a disadvantage in promoting preventive measures (Raman et al., 2023). However, in general, there is limited evidence that crackdowns by LEAs reduce overall market activity (Décary-Héty & Giommoni, 2017; Soska & Christin, 2015). Law enforcement interventions led in other cases to a decrease in the costs of illicit products and services, increasing the number of transactions conducted by vendors (Vana & Pachigolla, 2021).

The question of whether Telegram users exhibit similar behavioural patterns to those observed in dark web communities remains open in literature. However, empirical data can enable comparisons of criminal behaviour characteristics. For instance, user reactions to arrest news may reflect deterrence effectiveness. Indicators such as increased caution among users, behavioural shifts, mentions of relocating operations to more secure platforms, or a decline in message frequency after specific events would suggest that arrests influence criminal activity, even if only temporarily. Additionally, the data could reveal that some users are part of larger international organisations or indicate that Telegram's security is compromised, especially with data sharing in extreme cases, potentially reducing serious crimes. A notable difference may also emerge between the behaviours of oblivious and cautious

users. The dynamic between LEAs and criminals is likely to continue as a cat-and-mouse game (Soska & Christin, 2015), but examining this interaction could yield valuable insights.

4.1.2 Technology and Innovation

In recent years, the anonymity and security features offered by digital platforms have drastically transformed how individuals engage in criminal activities online. Platforms are being sought that are known to have minimal content moderation, or where such moderation is simply not feasible due to the encryption methods employed. Telegram, known for its one-to-one privacy features and decentralised structure, has become a hub for various forms of illegal and extremist behaviour. However, end-to-end encryption is not enabled in Telegram by default; this level of security is only enabled when both users in private conversations opt for full encryption. Many users mistakenly believe that this encryption happens automatically due to Telegram's 'safe' reputation. Consequently, numerous conversations in open channels remain accessible to law enforcement. Telegram has historically claimed that it refrains from extensive monitoring of its users, which has been confirmed in empirical research (Chayka, 2024). After facing criticism for insufficient content moderation practices, Telegram recently announced to share IP addresses and phone numbers with local law enforcement agencies and to increase moderation efforts, practices that had not been undertaken before (Roy et al., 2024; Telegram, n.d.-a; Wokke, 2024). While the lack of identity verification on Telegram allowed users to express radical views without fear of consequence, nurturing extremist ideology environments, the latest changes in the community guidelines of Telegram may propose positive change and have already led to an increased amount of blocked channels (Chua & Wilson, 2023; Telegram, n.d.-a).

As described earlier, technology and innovation have an important interplay with law enforcement interventions. The continuous evolution of law enforcement's digital surveillance techniques has driven criminal communities to improve their operational security. Telegram's and other decentralised platforms' commitment to privacy, as described by Chayka (2024), makes it a popular choice for criminals who seek a balance between ease of use and security (Frank & Mikhaylov, 2020; Wilson, 2020). The facilitation of illegal activities with minimal risk of detection on a significant international scale has consequently become more accessible through the global reach and lack of stringent identity checks by such platforms. Furthermore, it offers greater accessibility compared to marketplaces or forums found on the dark web, as it necessitates less prior knowledge regarding tech-savvy knowledge. In both cases, a sense of security under users is present due to relatively low detection risks. However, it remains unclear to what extent this perceived security influences adaptive behaviours among users. For instance, while increased law enforcement surveillance or platform policy changes may prompt some users to adopt stricter security measures or migrate to alternative platforms, others may continue their activities with little to no adaptation, relying on the platform's existing security features. Keyword monitoring for terms related to safety and encryption methods can indicate technological and behavioural adaptation.

4.1.3 Social Ties

User-to-user influence is, alongside the impacts from law enforcement and technology, an important factor contributing to exhibited adaptive behaviours of the *modi operandi* of underground community members. Understanding social factors provides valuable information about how these networks function and where their weaknesses lie. The identified factors can be subdivided into four main themes, namely: (I) Market Movements, Convergence and Economic Incentives, (II) Community Dynamics and Social Influence, (III) Reputation and Trust and (IV) Language Creation. First, the low cost of engaging in online crime compared to traditional offline crime significantly impacts offender behaviour. Digital environments lower barriers, such as physical risk and startup costs, leading to a more diverse offender pool (Baraz & Montasari, 2023). Many criminals adopt hybrid strategies, blending digital and physical markets, driven by economic considerations. Online crime's lower risks and higher profits attract offenders to migrate between markets. Vendors often engage in multihoming, operating across multiple platforms, maintaining ties with familiar partners, and adjusting pricing post-enforcement actions, further complicating interventions (Vana & Pachigolla, 2021).

Second, community structures significantly shape user behaviour. Norms and hierarchies often emerge through peer influence, with offenders relying on relationships within forums to maintain trust and share expertise (Chen et al., 2021). Debate exists regarding the strength of social connections in these communities. While some argue that virtual environments foster strong social bonds similar to physical networks, leading to normalised criminal activities Chua and Wilson (2023), others suggest these communities consist primarily of weak ties, making them susceptible to targeted interventions (Collier et al., 2022). However, mechanisms like hierarchies and reputation systems, often led by administrators or high-ranking vendors, promote trust and enforce norms, further reinforcing these networks' adaptability and resilience (Yip et al., 2013). Individuals who contribute valuable information can gain influence and deeper access to new communities, emphasising the importance of social ties and status (Mador, 2021). These dynamics align with social learning theories, where offenders model behaviours observed in their networks, with peers providing insights into market trends and risk assessment. Collective decisions, such as migrating to new platforms, are frequently driven by shared evaluations and mutual learning (Aldridge & Askew, 2017; Ouellet et al., 2022). For Telegram, it is hard to demonstrate whether users mutually trust each other, however, messages regarding collective platform migration could prove this to an extent.

Third, trust is a central concern in these anonymous environments. Given the constant threats from law enforcement and rival hackers, discussions around safety and security are prevalent. While users of darknet markets previously displayed some form of relaxed attitude, this has shifted '*to its current state of concern, uncertainty, and security-mindedness*' (Porter, 2018, p. S92). Fear is thereby not only expressed in the direction of law enforcement, but there is also an anxious attitude towards the possibility of hacks. In underground environments in the dark web, reputation systems, feedback systems, usernames and services like escrow stimulate trust, however, Telegram does not provide most of these features, meaning that trust must be established by different means, for example by reporting scammers to administrators or administrators using automatic deletion of chat messages after a set period (Devlin et al., 2024; Ladegaard, 2018; Mador, 2021; Roks & Monshouwer, 2020; Yip et al., 2013).

Language creation is the last factor that binds members within illicit communities. Unique terminologies, jargon and codes, different from English, are developed to distinguish insiders from outsiders, providing some kind of access control (Chua & Wilson, 2023; Hou et al., 2022; Mador, 2021). This specialised language creates a sense of belonging and loyalty while making communication less detectable to outsiders, including law enforcement.

4.1.4 Demand, Important Events & Media

The current demand ensures that providers of illegal products continue to innovate. For instance, the market for counterfeit documents has experienced significant growth, which can be attributed to the high demand and adaptability of the documents (Devlin et al., 2024). Frank and Mikhaylov (2020) underscore the interplay between product innovation and legislative constraints. As traditional drugs are increasingly criminalised, market dynamics and demand shift toward novel psychoactive substances, products designed to stay ahead of regulation, starting a (new) cat-and-mouse game between lawmakers and criminal networks.

Besides the interplay between criminal innovation, demand and law enforcement officials keeping up, an important role is assigned to social and political events. These occurrences, sometimes even unnoticed, influence the dynamics within criminal communities. During COVID-19, cybercriminals exploited vulnerabilities, targeting remote workers and pandemic-related fears with phishing schemes and fraudulent relief offers (Mador, 2021). The crisis also drove shifts in criminal behaviour, with lockdowns fuelling illicit activities and dark web engagement, from vaccine trafficking to the spread of misinformation, the pandemic diversified and intensified dark web activities (Raman et al., 2023). The impact of important events is further gained through the media, as trade volumes sometimes surge following media exposure, heightening vendors' sense of risk, and thus having opposite effects (Ladegaard, 2018). Even high-profile convictions failed to deter market activity. These operations and subsequent media stories may inadvertently publicise the platforms increasing the allure of these markets, for example by mentioning the profits or illicit products that are available, which could incite curiosity and attract new users (Jardine

et al., 2023). This is further complicated by how takedowns inadvertently inform users about operational security, making them more aware of future surveillance. Similar trends regarding Telegram could be anticipated.

These mentioned factors have played a significant role in criminal behaviour in dark net marketplaces. However, it remains the question whether these also have an effect in Telegram marketplaces. The presence of posts aimed at media exposure or current events may suggest that such activities influence behaviour.

4.2 Consequences and Impact on Criminal Behaviour

The various identified shifts in Telegram dynamics and the performed interventions have led to mixed outcomes. While some police operations, like Operation Onymous targeting Silk Road 2.0, have led to the temporary shutdown of major markets, the long-term impact remains debatable. Criminal markets display resilience, with vendors and buyers quickly migrating to new platforms after closure, showing signs of crime displacement and commoditisation.

4.2.1 Community Closure

Illicit marketplaces on platforms like Telegram and the dark web experience frequent change and innovation due to earlier mentioned external pressures. The relevance of this topic lies in understanding how criminal networks on Telegram adapt, reorganise, or relocate their operations when faced with these external pressures. By drawing on parallels with dark net marketplaces, insights can be gained into how these closures inform the resilience, adaptability, and innovation within illicit online communities.

Traditionally, the lifespan of darknet marketplaces has often been short, with many platforms closing soon after they launch (Devlin et al., 2024). The main reasons for these closures are intra-market disputes, hacker attacks, exit scams, and interventions by law enforcement. These factors make the environment highly unstable, with the threat of market shutdowns always present. Darknet market closures are often driven by operators' financial goals and risk reduction strategies. Once profitable, operators may shut down to avoid law enforcement (Y. Wang et al., 2023). Market lifecycles mirror regular economies, with rapid growth or declining vendor activity showing potential closures. Administrators may limit new vendors to reduce risks, but threats like DDoS attacks can still force closures.

Three types of market closure are often seen in dark net marketplaces, namely exit scams, voluntary closures and closure by law enforcement actions. The most common closure type for darknet marketplaces is the exit scam, where operators abruptly shut down and steal user funds held in escrow (Y. Wang et al., 2023). Since Telegram channels lack escrow systems, this form of closure is unlikely. In contrast, voluntary closures involve a more well-thought-out process. These types of closures are often announced early before they take place, allowing vendors and buyers to complete transactions (Y. Wang et al., 2023). While these closures were less common in the past, they have become more frequent as operators grow increasingly wary of law enforcement. Chen et al. (2021) point out that paranoia among market administrators can also drive voluntary shutdowns. Even suspicion of law enforcement infiltration can be enough to prompt a closure, causing effects as users move to other channels or platforms and improve their security measures. Within Telegram, creating or deleting a channel is remarkably straightforward, facilitating rapid changes in large channels where trading occurs. Finally, closures resulting from law enforcement actions are often the hardest to verify. Law enforcement agencies may sometimes take control of a market and operate it temporarily as a honeypot to gather information before shutting it down (Y. Wang et al., 2023). This can make it difficult to distinguish between voluntary (abrupt) closures and law enforcement takedowns, especially when agencies do not disclose their involvement.

An often-seen trend by criminals is multihoming, or cross-listing products across multiple platforms, mitigating the risks associated with shutdowns, which results in interdependent marketplaces. After an intervention, a short spike drop can be seen in goods exchanged, but this soon returns to previous levels or can even surpass the previous amounts of transactions (Décary-Héty & Giommoni, 2017; Ladegaard, 2019; Ouellet et al., 2022). This relocation to new platforms is called *crime displacement* and will be further addressed in the next subchapter. The communities are resilient and able to rebound, demonstrating a strong adaptability to external pressures. The question of whether

Telegram users show signs of these mentioned evasion techniques and the basis upon which a decision is made to terminate a marketplace is unknown in literature and will therefore be a point of attention for this study. Indicators of innovation might be evident if data analysis uncovers discussions about adopting new technologies, like encrypted communication apps or anonymity tools. Frequent mentions of updates on security practices or tips on avoiding detection may indicate a community's evolution to changing system environments. Furthermore, it is unknown to what extent Telegram vendors display forms of multihoming within Telegram. By being present in multiple channels and marketing in multiple places, shutdown risks can be mitigated, and the potential customer base can be increased. Studying this phenomenon within Telegram can reveal whether and how vendors diversify their operations to mitigate risks, a critical factor for understanding their resilience.

4.2.2 Crime Displacement

Closure of a platform does not imply that the criminal activity associated with it reduces. A common phenomenon is crime displacement where criminal activities shift from one platform to another (Moeller et al., 2017; Ouellet et al., 2022; Verburgh et al., 2018). Applying crime displacement as a lens enables the quantitative analyses to identify how the criminal ecosystem evolves when faced with disruptions, offering insights into patterns of migration, changes in operational methods, and adaptive strategies. These insights not only improve the understanding of criminal adaptability but can also be used for targeted interventions to disrupt displaced activities, rather than merely forcing them to evolve elsewhere.

Measuring this displacement has become easier due to the anonymous but transparent market properties (Van Wegberg & Verburgh, 2018). Being able to measure this in data allows for understanding the continuation of criminal activity in response to fluctuating dynamics within the systemic environment. While crime displacement in traditional drug markets has been researched often, translation to online environments, particularly illicit markets on Telegram, remains limited. Enforcement practices against darknet markets were still in an exploratory phase a few years ago, the same trend can now be seen regarding Telegram channels, partly because of the relatively recent emergence of these markets and the scarcity of enforcement actions targeted at them (Décary-Héту & Giommoni, 2017). The characteristics of online communities suggest that enforcement actions lead to shifts in crime patterns rather than a reduction in overall activity, altering the impact of police operations in size and scope.

The most common response to law enforcement pressure is tactical displacement, where participants alter their crime commission methods (Basheer, 2022; Décary-Héту & Giommoni, 2017). This could involve a shift from open to closed market operations, with dealers adopting innovative technologies. Another significant type of adaptation is geographical displacement, where activities move from one physical location to another. Research has indicated that law enforcement crackdowns do not necessarily reduce activity but instead prompt relocation.

Unlike the dark web, where switching platforms incur high costs and barriers thereby deterring less experienced participants, Telegram's user-friendly interface allows for rapid (internal) migration (Roks & Monshouwer, 2020; Vana & Pachigolla, 2021). This makes it an ideal environment for studying crime displacement and for understanding offender behaviour (Ouellet et al., 2022). Large-scale police actions have resulted in an initial drop in transactions and new vendor registrations, but the activity usually returns to previous levels within months (Décary-Héту & Giommoni, 2017). Two main effects explain this: a deterrent effect that temporarily reduces participation and a publicity effect that increases awareness of these markets (Jardine et al., 2023). Media is often likely to increase sales volumes, which can be seen in data from Operation Onymous, where some vendors were initially deterred, but media coverage helped the market rebound (Décary-Héту & Giommoni, 2017; Van Wegberg & Verburgh, 2018). This leads to a system that can become even stronger and more adaptable, thriving on disruptions (Jardine et al., 2023).

Considering the recent developments surrounding Telegram (i.e. increased moderating and sharing of personal data with LEAs) and the increased interest from law enforcement in conducting further investigations into the platform, it is relevant to explore the extent to which crime displacement occurs within this environment. It is

therefore essential to understand how measurement can be conducted in this context. Displacement within Telegram occurs when criminals adapt their operational methods, rather than abandoning the platform entirely. Instead of leaving Telegram, they may move to other public channels, from public channels to private invite-only channels or switch to direct encrypted chats. Although it is not entirely quantifiable, the opening and closure of channels or chat discussions regarding migration provide a clear indication of this phenomenon. This was also measured in earlier studies by either investigating vendor revenue or counting the number of vendors that moved to new markets after intervention based on their username (Décary-Héту & Giommoni, 2017; Ladegaard, 2019). While this generates generic results and provides a comprehensive overview of the entire situation, it is challenging to account for vendors who have completely ceased sales or those who have started using a different username, which could be needed to rebuild their reputation (Décary-Héту & Giommoni, 2017).

The prevalence of cross-posting products across channels or shifts in channel activity after major announcements could indicate displacement or resilience within Telegram. Tracking the timeline of these discussions can highlight how criminal activities shift in response to external pressures.

4.2.3 Commoditisation & Fragmentation

The commodification of crime can be seen as a structured economy, where criminals specialise in roles like credential theft or malware development (Mador, 2021). As Boersma (2023) and van Wegberg, Tajalizadehkhoob, et al. (2018) explain, this shift toward commoditisation has significantly lowered the barriers to entry for cybercriminals, as even those with minimal technical skills to engage in sophisticated (cyber)crimes by purchasing ready-made tools. Rather than building technical expertise or taking significant risks, criminals can now focus on making the right connections, thereby stimulating the growth of cybercrime (Kruisbergen et al., 2019). As a result, cybercrime is now characterised as *'specialisation and professionalisation, with individuals offering à la carte cybercrime services'* (Paquet-Clouston & García, 2022, p. 5). Combined with Telegram's ease of connecting with potential buyers, this creates a highly accessible platform for discovering new markets. This results in the creation of a cybercrime value chain, in which various service providers contribute to specific phases of an attack. Huang et al. (2018) compare this model to traditional business ecosystems, where each component adds value to the overall operation. These services range from vulnerability discovery to hacker coordination, customer support and outsourced DDoS attacks and cash-out services (Schrama et al., 2022).

The commoditisation of cybercrime allows criminals to outsource technical tasks, replacing expertise with the ability to purchase necessary tools or services, thereby accelerating cybercrime growth (Van Wegberg, Tajalizadehkhoob, et al., 2018). Anonymous online marketplaces are efficient venues for trading commoditised goods and services, reducing transaction costs and facilitating access (Van Wegberg, Tajalizadehkhoob, et al., 2018). At the same time, cybercrime communities are increasingly decentralised, fragmenting into smaller, harder-to-monitor channels (Hughes et al., 2024). This decentralisation complicates law enforcement efforts, as many channels require invitations or vetting, splintering rather than dissolving under pressure (Mador, 2021). The structured and commodified nature of the underground marketplace economy further reinforces this resilience, allowing even those with limited skills to participate in sophisticated criminal activities using readily available tools.

Indications of standardisation of products and services can uncover how commoditisation influences vendor behaviour and market patterns. For instance, commoditisation can lead to easier platform migration, a key element of tactical displacement. If vendors can replicate their operations across platforms or in other channels within Telegram with minimal effort, it highlights the role of standardised offerings in facilitating adaptation. In this context, Telegram presents a unique opportunity to explore how commoditisation manifests beyond traditional cyber-attacks. Analysing user messages for patterns like uniform product descriptions, standardised pricing, or discussions about ease of migration offers insights into the extent of commoditisation within this environment. Additionally, if messages frequently reference tools or services aimed at helping others engage in criminal activities, it confirms the presence of commoditisation-driven dynamics.

4.3 Conclusion

This chapter has provided an understanding of the interaction and dynamics between users and systemic dynamics, shaping criminal activities within Telegram channels, based on existing literature. This is mainly influenced by law enforcement actions, technological evolution, and user-to-user interactions, according to literature. This combination of factors creates a dynamic ecosystem where criminals adapt their *modi operandi* to exploit systemic weaknesses, technological opportunities, and social networks. Within these influences, various underlying factors are touched upon in literature. The most important insights for later stages of this research are summarised below.

Telegram's structural characteristics, including minimal regulatory oversight and ease of creating and migrating between channels, contribute significantly to its appeal for criminal activities and the continuity of crime. Law enforcement efforts, such as channel takedowns or arrests of key actors, traditionally created temporary disruptions while rarely leading to sustained reductions in criminal activity. Instead, these interventions often lead to reorganisation and migration, showing the resilience of criminal networks. The ability to migrate quickly within Telegram, supported by its user-friendly interface and search functionalities, contrasts with higher barriers to relocation in dark web markets, ultimately lowering the costs of adaptation for criminals and enabling them to maintain operations despite external pressures.

The interplay between technological capabilities and criminal innovation is exemplified by Telegram. While the platform lacks default encryption for public chats, its perceived security and low entry barriers make it a preferred choice for various illicit activities. Criminals exploit Telegram's secure characteristics to organise, advertise, and transact with minimal risk of detection. Commoditisation plays a central role in facilitating this adaptability. The availability of standardised tools and services enables even low-skilled individuals to participate in complex cybercriminal operations. This commodification accelerates the scalability of criminal activities and supports transitions between channels and platforms. For instance, the ability to replicate operations across Telegram channels reflects how commoditisation improves operational flexibility and overall resilience. These ongoing cat-and-mouse dynamics between law enforcement and criminal networks, where interventions often drive innovation rather than deterrence, are further displayed by new payment methods and innovation in product offerings.

Social dynamics within Telegram channels play a critical role in fostering adaptability among their members. Trust, peer influence, and shared norms enable responses to external threats, such as discussions about platform migrations or enhanced security practices. Contrary to other marketplaces, Telegram lacks built-in trust mechanisms like escrow services. Instead, users rely on features like auto-deletion of messages and administrator-controlled bots to maintain security and facilitate transactions. Specialisation further strengthens these dynamics, as individuals focus on specific crime categories, allowing them to develop expertise, improve operational efficiency, and build reputations within their niche. Telegram's role as a marketplace is further driven by its responsiveness to demand and the commoditisation of illicit services, such as cash-out solutions or fake documents, enabling rapid adaptation and market resilience. Media coverage and enforcement actions can deter participants temporarily but often inadvertently boost visibility and attract new users.

To sum up, existing literature identifies several key mechanisms that enable behavioural adaptation within illicit Telegram channels. The interplay between users' ingenuity, Telegram's favourable characteristics and criminal innovation (such as commoditisation), provides an environment where criminals can operate with a relatively low risk of detection. Continuity of channels is maintained through Telegram's decentralised structure and user-friendly interface, allowing quick migration and reorganisation when channels are shut down. This ensures that disruptions, whether from law enforcement actions or voluntary shutdowns, do not necessarily lead to long-term impact. When communities are ultimately closed, it is often unknown whether this stems from voluntary shutdowns, or shutdowns by LEAs. Commoditisation plays a crucial role by lowering entry barriers, and enabling even low-skilled individuals to access ready-made tools and services, which accelerates the scalability of criminal activities. Standardised products and allow vendors to replicate operations across multiple channels with minimal effort.

5 Setting the Context

The respondents from the semi-structured interviews represent diverse professional backgrounds, from knowledge centres and investigative services, offering distinct perspectives on the use of Telegram as criminal ecosystem, general observed *modi operandi* and broader insights into contemporary crime. The interviews aim to uncover key phenomena and practical experiences that can help interpret and contextualise the quantitative data analysis conducted later in this study. Given that each respondent specialises in different aspects of criminal behaviour and investigation, their perspectives complement one another. However, it is important to note that the interviews reflect individual viewpoints, and the findings should be viewed as illustrative rather than comprehensive or universally applicable. The derived insights are therefore presented as a coherent narrative, as contradictions or discrepancies in perspectives were not brought to light. Table 1 provides an overview of the roles and backgrounds of the individuals involved. All interviews were conducted physically, and the interview protocol, outlined in Appendix A, was used to guide the interviews. Individuals will be referred to in this chapter by a letter to ensure anonymity.

ID	Function	Background	Interview Length
A.	Expert Anti Money Laundering	Knowledge Centre	01h:05m
B.	Expert Financial Cybercrime	Investigation Service	00h:58m
C.	Expert Financial Cybercrime	Investigation Service	00h:47m
D.	Operational Specialist	Law Enforcement	01h:17m

Table 1: Interview Respondent Overview

Respondents A, B and C indicated that their work primarily involves conducting independent investigations or acting on tips received from other channels, with less focus on following up on reports of minor crimes. Respondent D is actively involved in investigating (online) crime, examining the identities involved and identifying larger networks. While cases from all respondents must have a connection to the Netherlands to establish jurisdiction, respondents emphasised that crime is often internationally organised and that they are often tipped by foreign authorities. In such cases, collaboration with international partners is essential. Investigations primarily target facilitators, being the key actors within the criminal supply chain, as focusing on these individuals can more effectively disrupt criminal networks: *‘Money mules won’t help you, they’ll find a new one in no time, you want to identify the coordinator’* (Respondent D, paraphrased).

During discussions, it became evident that the interviewed organisations cannot directly use data-driven methods, as employed in this research, without prior criminal suspicion and legal approval. As a result, investigations from respondents A, B and C often rely on tips or priorities set by management or political agendas. This focus can lead to certain types of criminal activity, including *modi operandi*, being observed more frequently. However, this does not necessarily reflect the actual prevalence of these activities in the broader landscape of crime. Instead, the heightened attention given to specific phenomena can create a perception bias in their analyses.

Respondent D’s situation is distinct. The team to which this individual belongs investigates a variety of criminal activities, including drug trafficking, lead trading, the exchange of explosives (such as heavy fireworks), and terrorism, all of which are connected to online communities. Notable cases have involved long-term undercover operations within Telegram channels, as reported by (Bosman, 2025), where actual agreements were made to purchase products, as well as extensive surveillance of drill rap groups and the associated exchange of weapons. Severe forms of crime, such as firearms, explosives, and lead lists, are hereby targeted. Lead lists are targeted because they facilitate other types of criminal activities. Explosives and fireworks are also prioritised due to their potential to significantly disrupt society and their use as weapons against law enforcement, particularly during events like New Year’s celebrations. In contrast, the trade of pharmaceuticals is less prevalent, as regulatory oversight for this area falls under other authorities. Incidents are addressed reactively when multiple reports have been received: *‘Before a trend catches our eye, people first have to report it, and then it’s: one report is coincidence, so is two, only from the third does it become a trend’* (D, paraphrased). Concern is expressed regarding future

trends of this situation, noting that law enforcement cannot adequately respond to these reports. These reports are typically received at a local level, which diminishes their visibility on a national scale. The phenomenon of mobile banditry among criminals results in a limited number of reports within the same region, as offenders frequently change locations in search of new, vulnerable victims. For instance, criminals involved in helpdesk fraud travel to the victim's location to collect bank cards or valuable possessions. Besides, this situation only becomes apparent when victims file reports, but feelings of shame often prevent this.

5.1 Use of Telegram

It is observed by all respondents that new communication channels, including Telegram, are routinely used for criminal purposes. Platforms are hereby sought from which it is known that the platform's regulation is insufficient, either intentionally or unintentionally. Without KYC, Telegram allows anyone with a phone number to create an anonymous account. The ease of obtaining anonymous prepaid SIM cards, which can be purchased with cash at small retail outlets, means that these phone numbers are frequently untraceable to individuals. Recently, Telegram has begun sharing these numbers and IP addresses upon request from authorities. It has been confirmed by respondent D that Telegram shares this information, however, the process of receiving it is lengthy as prosecutors and/or judges must grant permission for this, after which the request must be submitted. Nonetheless, this action serves as a deterrent, prompting criminals to explore alternative platforms that offer even greater privacy.

There is a significant variation in the ways in which criminals utilise Telegram, which can range from instances where a criminal has used Telegram to trade illegal goods while simultaneously using the same account to communicate for legitimate matters: *'We encountered individuals who were messaging their grandmother one minute, while selling criminal goods on the same phone in the same app the next moment. It really depends on how separate they keep everything'* (B, paraphrased). While some individuals employ it as a professional tool, many others use it simply for its convenience. Respondent D further indicates that other platforms that might look entirely unsuitable for illicit conduct, which feature integrated communication tools, such as online games (e.g. Call of Duty and Fortnite), there is a tendency to use these platforms for organising criminal activities and even discussing and virtually practising terrorism, due to their international communication facilitation, their accessibility and user-friendliness. For instance, Telegram has been employed for internal communication by groups like Extinction Rebellion and during the COVID-19 pandemic to coordinate (illegal) protests. This platform effectively diminishes geographical barriers and enables communication with unknown individuals: *'Crime looks so far removed, but it is secretly so close. Before, one needed a network with connections and the knowledge, now, with the rise of such platforms, that has become completely unnecessary.'* (D, paraphrased).

Most advertisements for offerings are posted in public Telegram channels. However, transactions typically move to one-on-one conversations, which can be encrypted if both parties enable this feature. Additionally, deals are conducted in private channels where more specific aspects of the transactions are discussed. Trust in public channels is generally low, as participants are often unfamiliar with one another. Access to private channels is typically granted only to individuals who have a person who vouches for them already present in the channel. Respondent D expects that these individuals know each other from earlier physical transactions and are already familiar before transitioning to closed channels. Consequently, the topics of discussion in these private settings differ from those in public channels, including the sale of raw materials, and the search for 'cooks', and supplies (e.g. kettles).

5.2 Modi Operandi

The experts have indicated that there are a significant number of trends identifiable in both current and emerging modi operandi. Given the impracticality of discussing and addressing all these trends, the focus has primarily been on identifying general observations, the factors that contribute to changes in modi operandi and the underlying reasons for their emergence. In general, it is observed that the use of digital platforms has led to a shift from traditional crime to digital criminality, displayed by increased exchange of counterfeit currency, fraudulent schemes,

cash-out operations, and lead lists. In this context, users typically sell temporary products that they currently possess, and which can be easily monetised. The digital nature of these transactions reduces physical interaction, making it easier to commit fraud, as victims are often unknown to the perpetrators. However, based on the insights of respondents B, C and D, it is challenging to categorise the individuals behind cyber- and financial crime, as they represent a cross-section of society. Nonetheless, it has been observed that more professional actors frequently employ runners who maintain contact with buyers and handle communication on these platforms. Subchapters 5.2.1 and 5.2.2 further address the underlying factors for differences in the used *modi operandi* under cybercriminals. Additionally, Subchapter 5.2.3 explores existing payment methods, the latest developments surrounding them and often-performed connected crime types.

5.2.1 Demand Identification and Recruitment

Criminal operations on Telegram differ based on organisational size and the segment of the value chain they occupy. Smaller-scale or *last-mile* activities often use Telegram for recruitment and communication, with participants serving as low-level executors rather than primary organisers. These transactions are often the visible tip of a much larger network. Telegram plays a key role in these networks, serving both as a recruitment tool and a communication platform. As an example, it is used for the recruitment of money mules and their mutual communication. Individuals, like students or minors, are hereby targeted and are willing to lend their bank accounts for criminal purposes, sometimes including schemes where individuals are tasked with purchasing luxury goods from retail stores, resembling Trade-Based Money Laundering (TBML). Telegram plays a two-fold role. First, a decentralised approach is used to minimise the visibility of the organiser. Instead of a single individual making large-scale purchases and attracting attention, tasks are distributed within a network to avoid detection. Telegram thereby acts as a communication platform between the executing members of the organisation. Second, platforms like Telegram play a role in their recruitment. Telegram's anonymity features help organisers stay hidden while coordinating operations, ensuring that those caught are typically low-level participants, leaving the broader network intact: *'The recruitment of money mules and other performers is often done via Telegram, as it protects the anonymity of the leaders'* (A, paraphrased). The recruiters are ruthless and unrestrained by social norms, and given the constant need for new money mules, it is anticipated that numerous cases regarding this type of crime will be found. In some cases, individuals positioned lower in the hierarchy can be used for the identification of crime facilitators, however, access to phone data is limited through the Landeck Ruling. Such access is now restricted to limited timeframes and particular applications, contingent upon justifiable cause and appropriate approval.

When the focus shifts to larger organisations, operations typically span multiple countries. For instance, respondent A references a UNODC (2024) report, which describes criminal compounds in Asia that conduct massive cyber-enabled fraud on a global scale. These cross-border structures affect the Netherlands through Dutch victims, Dutch money mules, and Dutch-language advertisements and help desks. With greater resources, these channels often have departments such as marketing, support, and web design, and may even employ AI to plan attacks with minimal human oversight. Although their Telegram use is not well-documented, it is plausible they rely on it in the final stages, for instance when coordinating with Dutch money mules.

5.2.2 Knowledge Level and Dissimilation of Expertise

In addition to utilising Telegram for exploring new markets or for recruitment purposes, there is a role for knowledge spreading. Experts frequently observe that criminals engage in discussions regarding the most suitable and secure communication channels. This includes sharing tips and tricks related to the purchase and use of PGP phones, as well as identifying when a previously used communication channel is no longer considered safe. It is observed that criminals' methods of operation adapt to areas where extensive knowledge is available. While this phenomenon is also observed in physical locations, such as the notorious Dutch 'Beverwijk' market, where licences and receivers for illegal IPTV are openly traded according to respondent C, online platforms are increasingly taking over this role.

Knowledge is simply shared by the individual who possesses it. When an individual with knowledge of prepaid credit cards operates within the network, other criminals are quick to adopt this method due to its ease and

accessibility. This highlights the collaborative nature of criminal networks, where members actively educate one another and share information to adapt their methods, which accelerates the spread of effective techniques within the network. The online dissemination of knowledge has hereby evolved into a business case. Not all knowledge is, however, shared. Individuals increasingly present themselves as professionals in specific domains, such as large-scale money laundering, depicting commoditisation. In the past, criminals were required to launder their own money and possess the necessary expertise to do so. Today, this process can be outsourced for a fee: *‘What I also noticed, and what can be seen as a trend perhaps, is that we are increasingly seeing professionals as intermediaries just really focusing purely on money laundering.’* (A, paraphrased). Consequently, most steps in the supply chain can now be delegated, if one has the right connections.

5.2.3 **Conventional Payment Methods Observations**

These different stages and sizes of criminal processes also propose shifts in payment methods, based on operational needs. Immediate and practical payments can be seen at the street level, while more sophisticated laundering techniques are observed by higher-level coordinators. Cash payments or payment services like ‘Tikkie’ (a popular Dutch peer-to-peer payment platform) likely occur within criminal environments. Such payment methods are most commonly observed in last-mile transactions at local levels. In these cases, transactions often involve physical contact for the exchange of goods, given the trade-based nature of the activity. As a result, physical payment methods are commonly used. Street-level criminals prioritise convenience, opting for the easiest and most accessible payment methods available. Once funds are generated through traditional criminal activities and aggregated by the crime coordinators, laundering becomes a priority. Even if the crime committed does not directly involve fraud or cash-out activities, such as cases where individuals commoditise one part of the value chain, subsequent cash-out processes are needed to convert the illicit gains into fiat currency.

Cryptocurrencies

Cryptocurrencies have grown rapidly in criminal use, driven by better accessibility, user-friendly exchanges, pseudo-anonymity, and increasing public interest. The scale of this growth was largely unexpected, and cryptocurrencies have now become accessible even to individuals with little or no understanding of their underlying principles. Despite initially negative associations (e.g. through ransomware), they have gained a broader appeal as an investment option. As a result, new crimes have emerged, including pig-butcher scams that lure victims into fake crypto investments. Thereby funds are lost via fraudulent platforms disguised as legitimate investment opportunities, never realising they are funding a non-existent venture.

Cryptocurrencies offer only partial anonymity. Large exchanges like Coinbase and Kraken have tightened KYC checks, making anonymous deposits or withdrawals more difficult. However, some platforms (e.g. Binance) historically had more lenient practices, allowing near-anonymous transactions. Current investigations focus primarily on facilitators within the cryptocurrency ecosystem, such as corrupt exchanges and cryptocurrency mixers, which help hide the origin of funds. One finding from these investigations is that large, compliant Dutch exchanges with robust KYC enforcement rarely, if ever, emerge as key players in criminal cases. Instead, the focus tends to be on international entities based in tax havens like Bermuda or Panama, where regulatory oversight is minimal.

Besides, criminals increasingly use cryptocurrencies for money laundering because transactions are cross-border, quick, and relatively cheap. They appear not only in cybercrime but also in off-chain offences like drug trafficking and fraud. As respondent A highlights, contrary to expectations, stablecoins have gained popularity for high-value transfers, as noted by Chainalysis (AMLC, 2024). Authorities can trace these coins on public ledgers using modern tools, but many countries lack specialised teams, creating global differences in enforcement capabilities.

A case which was referred to by respondents A, B and C is the takedown of a cryptocurrency mixer called ‘*Tornado Cash*’ (U.S. Department of the Treasury, 2022). Although the (Dutch) developer claimed that the tool was created for legitimate purposes, it was designed with criminal intent in mind, shown by its emphasis on providing maximum anonymity and advanced obfuscation techniques, without incorporating any features to enable identification,

monitoring, or enforcement (De Rechtspraak, 2024). Before this platform was taken offline, law enforcement became aware of the promotion of this platform on a forum, which was approached, informing them that promoting Tornado Cash could be seen as enabling criminal activities and could lead to prosecution. This preventive action prompted the forum to cease its promotion of Tornado Cash, demonstrating a clear deterrence effect. This case highlights the dual nature of cryptocurrency mixers. While they can serve legitimate purposes, such as improving privacy for legal transactions, they are also exploited for illegal activities. In many cases, platform hosts may be unaware of, or fail to investigate, the illicit uses of their services. After Tornado Cash was taken offline, however, other platforms with similar functionalities emerged, illustrating a clear waterbed effect within the criminal ecosystem (crime displacement). All respondents noted this displacement effect as a recurring phenomenon in their work, where the removal of one tool or platform leads to the emergence of alternatives. However, deterrence effects work for some users: *'Posting on a forum, for example, often works effectively, which can be as simple as: beware, you are being watched'* (C, paraphrased).

Cash, (Prepaid) Creditcards and 'Tikkie'

Cash is rarely used in criminal networks, partly due to Dutch regulations that limit cash payments to €10,000, soon dropping to €3,000. Storing large sums of physical cash is also impractical. As a result, prepaid credit cards, such as Paysafe, JetonCash, or AstroPay, have become popular for money laundering, since they can be purchased anonymously in small shops and are used both for transactions and as a form of salary for money mules. Beyond prepaid cards, criminals actively seek alternative methods to spend illicit funds using legitimate-looking payment cards. For example, there are reported cases of credit cards issued from non-EU countries with weak Anti-Money Laundering (AML) regulations and limited enforcement being used in the Netherlands. These cards offer relative anonymity and can hold substantial balances, making them attractive for large-scale spending without triggering immediate suspicion. Criminals also seek legitimate-looking cards from countries with lax AML measures, offering higher balances and greater anonymity.

In addition to cash and (prepaid) credit cards, previous research into illicit Telegram channels has revealed frequent use of the Dutch payment request service 'Tikkie.' Whether its use has changed over the years is unclear. However, expert B noted several limitations associated with Tikkie that constrain its suitability for large-scale criminal operations. For example, the maximum limit per request is €750, with a daily transfer cap of €2,500 per account. Additionally, Tikkie transactions are more easily flagged because they are tied to Dutch bank accounts and their strict KYC procedures. As a result, Tikkie is not practical for large-scale money laundering or ransomware attacks. Instead, it is more suitable for occasional transfers and (*last mile*) transactions involving individuals outside the criminal circuit.

Underground Banking

While not a formal payment method, underground banking was mentioned often during the interviews. Underground banking systems (also referred to as Hawala banking) remain a common method for moving funds internationally without relying on traditional banks or leaving a transaction trail. These systems are particularly attractive for specific types of crime. For instance, in drug trafficking, criminals often accumulate large amounts of cash that require immediate conversion and transfer. Underground banking allows them to quickly transform cash into value that can be moved across borders, often by investing in luxury goods such as watches or cars. These goods can then be transported and liquidated in other locations, further complicating detection and enforcement. Message platforms play a significant role in these operations, with messages containing amounts serving as informal ledgers to track debts or balances between parties. These interactions may occur in private, closed groups, but it remains unclear whether some of this activity is visible to outsiders who might lurk or monitor these conversations. This ambiguity adds another layer of complexity to efforts to monitor and disrupt these operations.

5.3 Conclusion

Using the interviews, the found concepts from literature can be contextualised and it is thereby possible to interpret quantitative trends in the next steps with foundational theories. The interviews delivered various key points. Below,

the most important insights for the remainder of this study, including crime specialisation, commoditisation and professionalisation, are elaborated upon.

First, Telegram has become a key platform for cybercriminal activities due to its ease of use, anonymity features, and global reach. However, its role is evolving as law enforcement increases its attention. Recent developments, such as Telegram sharing user phone numbers and IP addresses with authorities, is anticipated to push criminals toward alternative privacy-focused messaging platforms (e.g. Signal) or online gaming environments (e.g. Fortnite). Criminals thereby tend to choose the easiest and most familiar platform available to them. While some operate in professionalised networks, others engage in crime opportunistically while maintaining everyday use of these platforms, combining legitimate and illegal activities on the same account, making it even more difficult to distinguish between regular users and criminal actors. A key challenge is anticipating criminal migration patterns. When one tool or platform becomes unsafe, criminals quickly shift to alternatives, leading to crime displacement rather than elimination. While it remains uncertain how criminals can be forced to discontinue their criminal behaviours, preventive strategies, such as warning messages and deterrence efforts, have shown effectiveness in disrupting criminal activity, as seen in the case of 'Tornado Cash'.

Second, the interviews have revealed that crime is increasingly moving to online worlds, with fraud, cash-out schemes, and fake investment scams taking over traditional organised crime. Telegram plays a crucial role in this shift, particularly in recruiting money mules and coordinating financial crimes. Criminals exploit the platform to find individuals willing to move funds and organise operations across multiple accounts and channels. The shift to digital crime should be observable in several observations within Telegram. Messages targeting money mules, high-frequency users who operate across multiple groups, indicating facilitator roles and criminal collaborations between different Telegram channels could prove this. Simultaneously, law enforcements have a lack of resources to track and arrest all low-level offenders involved in these schemes. Instead, efforts focus on identifying and disrupting key facilitators, who organise, finance, and connect criminal networks.

This shift in digitalisation is also anticipated concerning payment methods. Criminals use different payment methods depending on their level of operation. Street-level criminals prefer cash, Tikkie, or prepaid credit cards for small, local transactions where physical goods are exchanged. Higher-level coordinators rely on cryptocurrencies and underground banking for money laundering and international transactions. It is anticipated that criminals choose the preferred method of payment based on what is available and what they are familiar with. However, criminals may use multiple payment methods as a risk management strategy. Enabling the possibility to discover a link between often-used payment methods and offered types of crimes. Vendors with more accepted payment options may be more professionalised, suggesting that analysing payment diversity could indicate a vendor's level of experience and specialisation. The growing accessibility of cryptocurrency has further enabled scams like pig-butchering schemes, where victims are lured into fraudulent crypto investments, surging the number of cybercrimes.

Last, besides the use of Telegram for finding and communicating with (new) demand and recruitment for staff and money mules, it is often used for sharing knowledge regarding tools, enforcement evasion tactics and new crime methods. A key observed trend is the commoditisation of cybercrime services, where expertise is monetised through guides, courses, and APIs for automating illicit activities, making cybercriminal ecosystems more scalable and professionalised. This rapid knowledge sharing accelerates criminal innovation, making it harder for law enforcement to keep up. While some share insights freely to protect themselves, many sell their expertise, particularly in high-value areas like money laundering and underground banking. The presence of knowledge exchange in chat messages, advertisements of crime services (like laundering or fraud automation) and telegram actors that specialise in executing specific segments of the supply chain indicate that commoditisation extends beyond initial expectations.

6 Detailed Quantitative Approach

Chapter 0 has outlined the rationale for the selected quantitative methods. Given the sequential application of various methods, where data from prior analyses is utilised to derive new insights, this process warrants further clarification. Therefore, Figure 2 presents the research flow diagram, which shows all intermediary steps, the input and output of data, as well as the overarching insights derived from the analyses. Each method, including taken design choices, is further explained in this chapter.

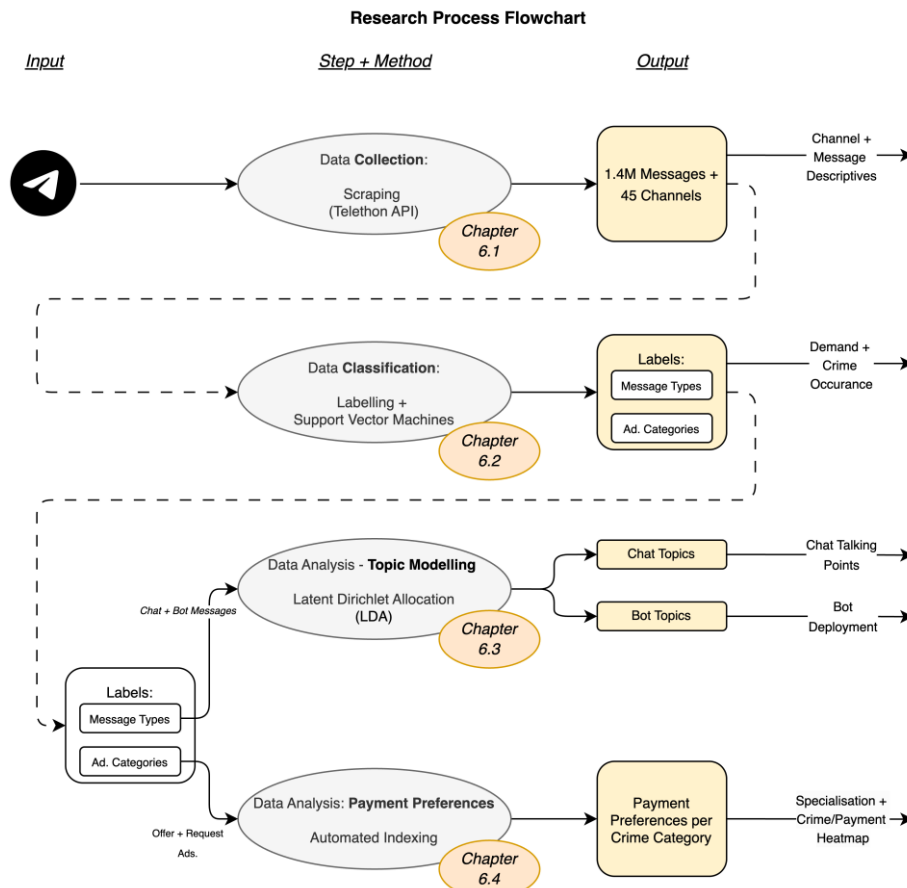


Figure 2: Research Process Diagram

6.1 Scraping: Telethon API

The process of identifying appropriate Telegram channels, following the criteria outlined in section 3.3.2, proved to be a time-consuming task as this had to be done manually as it is challenging to automate effectively. Finding suitable channels involved a combination of targeted keyword searches and a snowball sampling method. Starting with independently identified channels using Telegram's manual search function, the research also used Telemetrio, an analytics service for businesses on Telegram, to identify (illicit) marketplace channels (Telemetr.io, n.d.). This served as a foundation for locating relevant channels after which the snowball sampling method was used, where shared URLs to other Telegram channels were followed and reviewed for suitability. Considerable time has been dedicated to this manual search for groups.

A total of **45 eligible Telegram channels** were identified for analysis. While this likely includes only a subset of the Dutch public criminal ecosystem on Telegram, it provides a robust sample. These channels include all major categories of crime, characterised by a sufficient volume of messages, sufficient activity over time, and a substantial number of contributors and subscribers. Together, these factors ensure that the dataset reflects the broader dynamics of Dutch criminal behaviour on Telegram. The analysis also includes channels that appear to be legitimate but simultaneously offer illegal products or services. For instance, users of legitimate channels may list items such as cars and motorcycles, accompanied by the phrase 'zonder 123' (English: 'without 123') in their descriptions,

indicating that the product lacks the legally required identification number or that the product is sold without a registration certificate or keys. From the identified channels, data was extracted using Telethon API, an open-source Telegram scraper, which has been modified (Cugler, 2024). The existing code was improved with new functionalities, including improved preprocessing and exporting, a backup saving mechanism. Additional preprocessing was necessary for unstructured data from these sources, addressing issues like emojis, long messages, and unusual formatting. Emojis were converted to Unicode for analysis, unsupported characters and HTML tags were removed, and all text, including stop words, was preserved. Scraped data includes channel names, author IDs, message content, timestamps, and metadata like views and shares, excluding media files. To comply with Telegram's API limits and avoid detection, scraping was capped at 1,500 messages per API call, with delays to mitigate Floodwait errors. Measures to maintain anonymity included using a dedicated phone, an anonymous SIM card, a VPN, and an untraceable screen- and username ('Deleted Account').

By strategically sequencing the groups during the scraping process, further optimisation was achieved, allowing for the scraping, processing, and storage of up to 120,000 messages per hour. This entire procedure took 14 hours and resulted in the collection of 1,477,606 messages sent between **20-02-2021 and 20-11-2024**, contributed by **14,856 users**. During preprocessing, it was noted that numerous messages consist solely of images, videos, or voice memos showcasing goods for sale, without accompanying text. Including these messages in the analysis posed significant challenges, such as slowing the scraping process, increased detection risks by Telegram, and complicating data integration. Therefore, these non-text messages were excluded early in the data preprocessing stage to streamline the analysis. Ultimately, a total of 87,982 (5.9%) empty messages were filtered out from the dataset, leaving **1,389,624 messages** available for further analysis. As the report by Schrama et al. (2022) can be used as a reference framework, it is possible to compare descriptives about the scraped Telegram messages, which is presented in Table 2. It reveals a notable decrease in the number of messages sent (or the possibility of an increased number of deleted messages) in the current dataset. Besides, the current dataset appears to exhibit a relatively lower occurrence of empty messages, such as images and videos lacking accompanying text. However, both the average and the median of sent messages across the channels are lower than those observed in the reference dataset. This discrepancy cannot be accounted for based on the number of scraped groups or the duration of the study period, as this is comparable with the reference dataset.

To prevent potential misuse, the names of the Telegram channels labelled in this research are not disclosed. Instead, each channel has been assigned an alias derived from an observation of the most often exchanged goods and/or services. These references to the groups will be used throughout the remainder of this report.

	Current Dataset	Reference Dataset
Number Of Channels	45	48
Scraping Period	20/02/2021 - 20/11/2024	15/01/2017 - 19/02/2021
Max. Messages In 1 Channel	228,185	412,098
Channel Average	32,835	81,594
Channel Median	3,207	42,976
Number Of Messages Scraped	1,477,606	3,916,558
Number Of Empty Messages (i.e. Picture-Only)	87,982 (5.9%)	637,231 (16.3%)
Remaining Messages for Analysis	1,389,624	3,279,327

Table 2: Comparison of Descriptive Statistics between Current Dataset and Reference Dataset

Rather than focusing solely on the groups that could be scraped, it became apparent that several groups went offline before their data could be scraped. Between September and early November, 26 market channels either ceased operations or were made private, coinciding with Telegram's announcement to share phone numbers and IP addresses with authorities upon request and improved moderation efforts (Telegram, n.d.-a; Wokke, 2024).

Among these 26 closed channels, 12 were general channels, 5 were drug-related, 1 focused on local trade, 6 facilitated cashout operations, 1 dealt in firearms, and 1 specialised in fireworks. It is hereby expected that channel closure primarily involves more serious types of crime, as authorities are likely to request data specifically from individuals engaged in these more severe offences, such as arms trafficking and child pornography. In addition to the channels that could not be scraped, seven other markets were shut down completely during the writing of this report. Seven channels closed without further explanation, one channel had the following message displayed: *'This channel can't be displayed because it violated Telegram's Terms of Service'*. Furthermore, one was temporarily suspended by Telegram: *'This group has been temporarily suspended to give its moderators time to clean up after users who posted illegal pornographic content. We will reopen the group as soon as it complies with the Telegram Terms of Service again.'* The seven markets that completely ceased operation focused on weapons (1), local activities (1), cash-out (1) and general offerings (4). These channels, with nearly 220,000 messages, have contributed significantly to the formation of the current dataset. In conclusion, of the 71 identified channels that fulfilled the set criteria of this research, only 38 were still active early February 2025.

6.2 Labelling and Classifying: Annotation and Support Vector Machines

Labelling

The Telegram Classifier, adapted from Schrama et al. (2022) which proved to work effectively, in combination with the PigeonXT library (Python 3.9.20 in a Jupyter Notebook), was used to label new messages. Before labelling, empty messages (those containing only media) and duplicates within channels were filtered out to prevent frequently occurring messages from overshadowing the labelling of unique messages. Labels were then manually assigned, and the results were saved in a new pickle file for subsequent analysis.

The first classifier categorised messages into four distinct types. First, messages were evaluated to determine if they were advertisements. If an individual offered or promoted a product or service, the message was labelled as 'Ad. - Offer'. If an individual requested an illegal good or service for purchase, it was labelled as 'Ad.- Request'. Non-advertisement messages were categorised as either 'Chat Messages', representing general discussions, or 'Bot Messages', which included automated updates from Telegram bots (e.g. member joins, warnings, or bans). Each message was assigned a single label, ensuring mutually exclusive categorisation across these four types. Table 3 presents actual anonymised (Dutch) Telegram messages as examples in their belonging category.

Ad Type	Example Message
Ad. – Offer (see Figure 1, Figure 13, Figure 14, Figure 15)	<i>'We hebben weer ingeslagen op sloffen sigaretten aangezien de prijs van de sigaretten duurder zijn geworden. Wil je niet meer de jackpot prijs betalen in winkels bestel dan bij ons! Prijzen: (10pakjes van 20), 1Slof=40eu, 5Slof=150eu, Meer? Onderhandelbaar. 🚚: levertijd max 2 dagen na betaling met Track en trace! 📱: betaling via Tikkie, Paysafe Geïnteresseerd? pb dan @##### Ook nu camel en chester sloffen beschikbaar!'</i>
Ad. – Request	<i>'🔥 dringend koeriers gezocht 🔥 MET EIGEN WAGEN! 7/7 beschikbaar kunnen zijn! Werkuren zijn van 13u30 tot 12! €2500 tot €3000 per week gegarandeerd! Je krijgt dagelijks BETAALD! Enkel serieuze werkers gezocht die willen knallen 📱. Je levert enkel aan nette vaste klanten! Interesse? CONTACT : @#####'</i>
Chat Message	<i>'##### apotheker is oplichter trap er niet in als je shag moet hebben'</i>
Bot Message	<i>'User ## is banned in the current federation (##) and so has been removed. Reason: scam'</i>

Table 3: Available Message Types with Example Text

In addition to the message types, messages labelled as Advertisement (including both 'Offer' and 'Request') are evaluated based on the category to which they belong. Unlike earlier labelling, messages may now fall under multiple categories; for instance, if a message includes various types of criminal activity simultaneously. Earlier work in this field mostly put the point of attention on one certain type of crime per study, such as the offering of cybercrime commodities or the exchange of drugs (Van Wegberg et al., 2020). It is now essential to obtain a complete understanding of the entire criminal ecosystem; therefore, all known crime types are utilised in the labelling process. To be able to apply previously labelled data to the current dataset in a later phase, an assessment was

conducted to verify the completeness of existing categories in similar research (e.g. Schrama et al., 2022; Boersma, 2023). While the established categories proved complete, new products within these categories were observed, including vapes, SIM cards, drug production materials, illegal IPTV services, anabolic steroids, and recruitment of (underage) money mules. Table 4 provides a non-exhaustive summary of identified advertisement categories.

Ad Categories	Breakdown
Weapons	- Knives, Tasers, Brass Knuckle etc.
Firearms & Explosives	- Guns, Explosives, Munition etc.
Soft Drugs	- Soft Drugs (e.g. Weed, Hasj, Cigarettes, Alcohol, Vapes), - Materials to Produce Soft Drugs (e.g. Cannabis Plants)
Hard Drugs	- Hard Drugs (e.g. Cocaine, Heroin, XTC, MDMA, GHB), - Materials to Produce Hard Drugs (e.g. GBL)
Pharmaceuticals	- Medication (e.g. Xanax, Oxycontin, Morphine), Anti-depressants, Erection Pills (e.g. Viagra), Sleeping Pills, Anabolics
Cybercrime	- Phishing Panels, Hacking, Digital Scams, Sim Cards, Digital Subscriptions (e.g. Netflix, Thuisbezorgd, Instagram, Snapchat)
Licences & Personal Documents	- Forfeited or Cloned Documents (e.g. Driver Licences, Passports, Certificates of Good Conduct, Diplomas)
Fireworks	- Illegal fireworks
Cashout	- Fraud, Money Laundering, Gift Cards, Stolen or Cloned Credit Cards - Recruitment of Money Mules
Stolen Goods	- Stolen Goods (e.g. Cars, Motorcycles, Bikes, Electronics) - Forfeited Goods (e.g. Designer Clothing, Watches)
Other	- Prostitution & (child) Pornography, IPTV, Matchfixing, Cabs, Manpower & Labour

Table 4: Available Advertisement Categories, adapted from Boersma (2023)

During the labelling process, several challenges emerged. The first notable issue was the frequent occurrence of messages that offered multiple types of criminal activities simultaneously, such as the promotion of soft drugs, hard drugs and pharmaceuticals, or the combination of cybercrime and cash-out solutions within a single message. In these instances, all relevant categories were assigned to the messages. Secondly, some messages contained text that was highly cryptic, often serving as a secondary element to accompanying images or videos. Relying solely on the text made it difficult to definitively ascertain the category being offered; however, the literal wording was utilised as the determining factor. Thirdly, slang was often used in the chats, which meant that forums and urban dictionaries needed to be consulted before messages could accurately be labelled. Lastly, certain product categories posed challenges in determining their appropriate classification, particularly in cases involving the offering of bank accounts or gift cards, which could be categorised under both cash-out and cybercrime in several cases.

Selection of Labelled Messages

The goal of the classification model is to accurately predict the types and categories of messages. As outlined in Chapter 3.3.2, at least 0.5% of all messages in the dataset need to be labelled for the model to perform effectively. Given the availability of a high-quality, pre-labelled dataset that met the specified requirements, it was not necessary to manually label the entire set of messages. Therefore, to meet the labelling target, the design choice was made to manually label 0.2% of the messages. The remaining labels were supplemented with the available pre-labelled data to reach or exceed the 0.5% threshold, depending on which combination yielded the most effective predictive model in subsequent stages.

For the manual labelling, semi-proportionate sampling was employed, where the sample size for each stratum is deducted from the overall population of messages. However, it is also crucial to obtain enough labelled messages from smaller Telegram channels. Consequently, at least 80 messages per channel were labelled, or fewer if a channel had limited unique messages. An upper limit of 325 was set, although only two channels required such a

restriction. Importantly, only unique messages were labelled per channel to prevent the labelling of messages that were frequently sent. This process ultimately resulted in 3,873 independently manually labelled messages, which took 16 hours to complete accurately. Table 5 presents an overview of the distributions of these messages.

Ad. Type		Ad. Category	
Ad. – Offer	58,4%	Weapons	0,3%
		Firearms & Explosives	3,3%
		Soft drugs	25,6%
		Hard drugs	26,0%
		Pharmaceuticals	9,5%
Ad. - Request	15,1%	Cybercrime	7,8%
		Licences & Personal Documents	3,4%
		Fireworks	3,7%
		Cashout	15,8%
		Stolen Goods	5,0%
		Other	6,0%
Chat Message	12,3%		
Bot Message	11,8%		

Table 5: Manually Labelled Types & Category Distribution

Assessing the extent to which the earlier-mentioned complexities have resulted in mislabelling messages is challenging. It is assumed that the use of slang and the fact that some messages offered multiple categories had limited impact, as additional time was spent ensuring accuracy and making well-informed decisions. However, labelling cryptic messages, especially those lacking accompanying media (which were not available), may have led to errors. To estimate the margin of error, all manually labelled messages with fewer than 20 characters were identified. This amounted to 342 messages out of the 3,877 total manually labelled messages. While many of these short messages contained clear indicative terms such as 'Coke', 'Snus', or 'Stolen 🚗', a significant proportion lacked context and did not indicate the message type or category of criminal activity. It is estimated that roughly one-third of these short messages fall into this ambiguous category. Assuming a relatively high error rate of 50% for these ambiguous messages, the overall error margin across all labelled messages is calculated to be 1.47%. In practice, however, the actual error rate is likely higher due to additional factors, including fatigue during the labelling process, ambiguity in category definitions, and the nuanced use of slang. Quantifying the exact impact of these factors remains difficult, but they underscore the challenges of manual labelling in this context.

After labelling the messages, two scenarios were developed. In Scenario A, approximately 0.35% of pre-existing labelled messages were added to the dataset, resulting in 8,713 labelled messages (0.63% of the dataset). A design choice was made to maintain the proportions of crime categories (based on the distribution in Table 5), even though this limited the balance between message types (advertisements, chat, and bot messages). However, this approach had skewed results during testing due to the low number of labels in certain categories, leading to errors in model training. Therefore, *Scenario B* was chosen, where the manually labelled messages were supplemented with the full set of pre-existing labelled messages, resulting in 22,543 labelled messages (1.62% of the dataset). Based on evaluation criteria, which are explained in upcoming paragraphs, *Scenario B* was selected due to its robustness and reliability, and several other advantages. First, a larger dataset was used for training, which is beneficial for capturing nuances in complex data. Second, it provided improved reliability and the potential for better distinguishing nuance between message types. Last, it aligned better with best practices, which recommend using as many labelled data points as possible when available.

Assessing

Before assessing the model's performance, the tools for evaluation are first outlined. The input parameters are optimised individually to create the best possible predictive model, ensuring the most effective combination of

settings is identified. To maintain consistency, the random number generator remains fixed, ensuring that messages are divided in the same way during each evaluation. This approach also supported the decision to select *Scenario B* as the preferred dataset. To evaluate the performance of the SVM algorithm, confusion matrices are analysed alongside precision and recall scores, providing an assessment of the model's accuracy and its ability to correctly classify messages. This is a tool used to evaluate the performance of the classification model, providing a detailed breakdown of predictions into four types: True Positives (TP), False Positives (FP), True Negatives (TN), and False Negatives (FN). By organising predictions in this way, the confusion matrix offers insights into the model's ability to classify messages accurately. It highlights not only the number of correctly classified instances but also reveals patterns in misclassification, showing which labels are confused with others. From the confusion matrix, key performance metrics like precision and recall are derived. Precision measures the accuracy of the model's positive predictions, answering the question: 'Of the messages classified into a specific category, how many truly belong there?' High precision for a label ensures that the model minimises false alarms. On the other hand, recall, or sensitivity, evaluates how well the model identifies all relevant instances in a category. It answers: 'Of all the messages that truly belong to this category, how many were correctly classified?' High recall for a label ensures the model captures most of such messages, even if it occasionally includes false positives. Balancing precision and recall is essential for creating a robust classification model. To optimise both metrics, the SVM parameters were carefully hypertuned through iterative adjustments.

Preprocessing and Model Parameters

To prepare the data for the SVM model, text was lowercased to ensure uniformity, numbers were removed, and both single words (unigrams) and two-word combinations (bigrams) were used as features. The Term Frequency-Inverse Document Frequency (TF-IDF) method was applied to emphasise rare but meaningful words. The SVM model, using the scikit-learn library, was trained using the hinge loss (commonly used for linear Support Vector Machines) and the *L2 Penalty* (default) (which penalises large weights, reducing the risk of overfitting and improving generalisation) (scikit-learn, n.d.). The model was trained on 80% of the labelled data and tested on the remaining 20%, a commonly used split for optimal accuracy (Satrya et al., 2022).

To confirm the suitability of SVM for this task, its performance was compared to Naive Bayes and Random Forest models. SVM outperformed both, achieving a precision of 91.3%, compared to 80.2% and 72.1% for Naive Bayes and Random Forest, respectively. While a chi-square test was considered to evaluate the association between observed and predicted distributions, it was determined that such a test would not provide conclusive insights given the dataset's composition. The SVM model was ultimately validated as the most effective approach for this analysis.

All channels have been assigned an alias, and with the manually labelled messages, the support vector machines were trained. The first classification model classified the type of message ('Ad. – Offer', 'Ad. – Request', 'Chat Message' and 'Bot Message'). The amount of offers ads was too substantial, therefore, the design choice was made to downsample it, proportionally to the smallest group, as it might otherwise skew the results of the SVM model (Lee & Seo, 2022). Additionally, '*class_weight=balanced*' was used to further mitigate the imbalance. This ensures that minority classes have more influence during training, improving their representation in the decision boundary. As a result, nuances in the smaller categories (chat messages and bot messages) are better captured.

The model relied on several key parameters to optimise its performance. One of these was *alpha*, which controls regularisation strength. Higher *alpha* values impose stricter regularisation, preventing the model from overfitting by prioritising simplicity over closely fitting the training data. Another important parameter was *max_iter*, which sets the maximum number of iterations the algorithm uses to refine its weights and minimise the loss function. To ensure reproducibility, the random state was kept fixed throughout the training process. While the default parameters in SVMs are generally effective for text classification tasks, a grid search was conducted to explore potential improvements (Sebastiani, 2002). This involved testing alternative values for parameters such as *alpha*, the maximum iterations, the *n-gram range*, and whether to toggle TF-IDF. In particular, increasing the maximum number of iterations proved beneficial when working with complex, non-uniform data.

The second SVM model focused on predicting the 11 advertisement categories, following a similar setup to the first, however, due to the reduced number of absolute labels in some categories and the possibility of reduced predictability power, downsampling was not used. For both models, the impact of altering the training/test data split was investigated. While the standard 80/20 split provided consistent results, a 70/30 split was tested to increase the test set size for underrepresented categories. However, this adjustment reduced overall model performance, affirming the effectiveness of the original split. Last, a grid search was conducted to determine if the model's parameters could be hypertuned. It was found that increasing the maximum number of iterations and reducing the 'clf_alpha' parameter improved the model's predictive performance. Setting the iterations to 100 allowed the model to take more steps toward convergence, which was particularly beneficial for complex datasets and scenarios with smaller learning rates. A lower 'clf_alpha' helped to achieve a better balance between underfitting and overfitting.

Classification Performance

The 'message type' prediction model achieved a model precision of 84.8% and a recall of 85.3%, which is comparable to, or higher than, reference studies using the same method (Schrama et al., 2022; Van Wegberg, Tajalizadehkhoo, et al., 2018). Figure 16 in Appendix D presents the confusion matrix, which shows that the predictive performance for messages labelled as 'Ad. – Offer' and 'Bot Message' is exceptionally high (above 0.9). However, it is notable that a relatively large number of messages that are actually request advertisements are misclassified as offer advertisements. This misclassification does not pose significant issues for subsequent analyses. The model also struggles to distinguish chat messages from advertisements (of both types). Manual re-evaluation of labels confirmed consistency in the labelling process, ruling out discrepancies as a cause of poor classification. This discrepancy was even more revealed in other scenarios with different amounts of added labelled messages and was also observed in the reference dataset, which encountered similar challenges.

Ultimately, it was found that 80.9% of the dataset consisted out of offer advertisements. This high number of offer advertisements in the population seems greatly higher than the distribution in the manually labelled messages (as shown in Table 5 on page 37). This discrepancy can be explained by the fact that a unique message was only labelled once during manual annotation, which was a deliberate design choice. This predominance is also reflected when Telegram channels are analysed by message type. Figure 3 presents the distribution of message types per channel, focusing on channels with more than 30 messages. This analysis reveals that only a few channel administrators make frequent use of bot messages. Additionally, the presence of chat messages or offer advertisements varies significantly between channels, with not all four categories appearing on every channel.

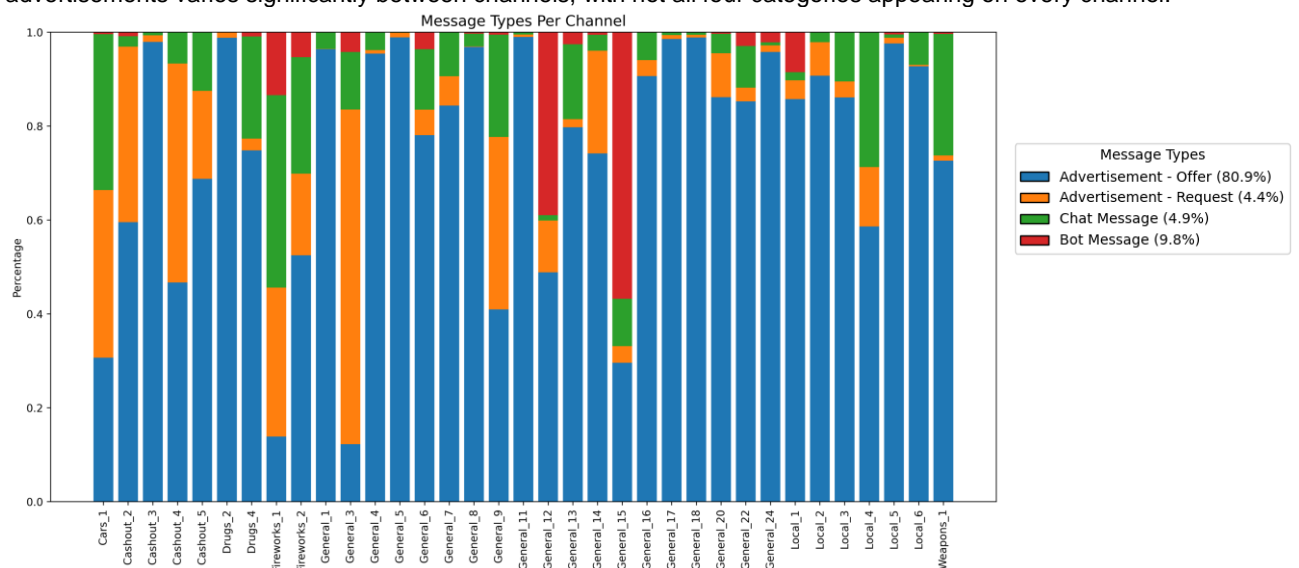


Figure 3: Message Types per Channel

The second SVM classification model reveals a significant disparity in the number of advertisements across crime categories, as displayed in Figure 4. Pharmaceuticals (28.0%), soft and hard drugs (11.2% and 22.9%), documents

(11.0%), cybercrime (9.7%), and cashout (11.2%) are heavily advertised, whereas weapons, firearms, and fireworks appear far less frequently in the analysed advertisements. The model achieved a precision of 84.1% and a recall of 76.1%, which aligns with the results of previously conducted studies. Figure 17 in Appendix D presents the confusion matrix for this model, showing that all advertisement categories with good accuracy (above 0.8), except for the weapons category, pharmaceuticals, stolen goods and 'other'. The lower predictive accuracy for *pharmaceuticals* can be attributed to the frequent bundling of these items with soft and hard drugs in advertisements, leading to overlapping categories. Similarly, the lower predictive accuracy for *weapons* is due to the small number of labels available in the dataset, making it more challenging for the model to reliably identify this category. Manual analysis of the *stolen goods* and *other* categories revealed significant variation in the items offered or requested, and occurred infrequent in the dataset, contributing to lower prediction power for these categories.

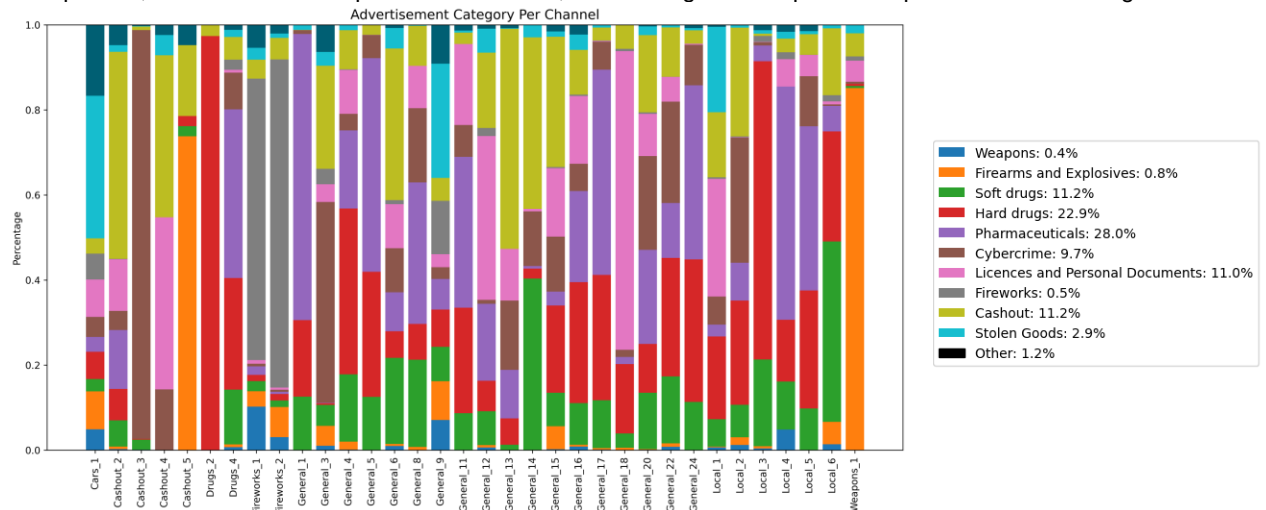


Figure 4: Advertisement Categories per Channel

Through manual analysis and examination of the raw data from the channels and messages, it became evident that a large number of identical messages are being sent in the channels. Using insights from the first SVM model, it is feasible to determine the number of unique messages present in the dataset for each message type. This process involved counting unique messages per author for the two datasets. Consequently, if multiple authors send the same message (which is quite common in messages with label 'Chat Message'), that message is counted multiple times. The percentages of unique messages were calculated by dividing the number of unique messages by the total number of messages identified within that category. The insights can be found in Table 6.

	Current Dataset			Reference Dataset		
	Unique	Total	%	Unique*	Total*	%
Total	73,186	1,389,624	5,3%	853,370	3,916,558	21,8%
<i>Ad.- Offer</i>	27,588	1,123,933	2,3%	251,204	1,832,446	13,7%
<i>Ad. - Request</i>	18,716	61,519	30,4%	242,933	779,065	31,2%
<i>Chat Message</i>	17,649	68,443	25,8%	336,885	1,226,895	27,5%
<i>Bot Message</i>	9,233	135,729	6,8%	22,348	78,152	28,6%

Table 6: Unique Messages per Message Type in Current Dataset and Reference Dataset

The insights derived from the table above will be utilised in Chapter 7.1 to analyse the results concerning the (differences in) usage of Telegram across the two datasets. It is important to note that, unlike this research, which does not classify empty messages, the reference study has included such classifications. Consequently, the total number of messages, as well as the counts within the message types, deviates from what would be anticipated.

6.3 Topic Modelling: Latent Dirichlet Allocation

Latent Dirichlet Allocation (LDA) was used to analyse large volumes of messages and identify underlying topics. The analysis was conducted twice on the current dataset, focusing separately on *Chat Messages* and *Bot*

Messages. This subsection will delve deeper into the utilised approach employed for these analyses, the optimisation of the model, and the number of latent topics identified.

Model Parameters

The LDA's are performed using the Gensim LDA library, as it is faster and more deterministic for large datasets than other libraries (i.e. MALLET), making it ideal for exploratory analyses. To ensure reproducibility, the LDA algorithm was run on a single CPU core, avoiding variability introduced by parallel processing (Ebeid & Arango, 2016). The analysis began with preprocessing by removing numbers, accents, and short words, as well as tokenising the messages. Dutch and English stop words were filtered out using NLTK to ensure only meaningful words were analysed. These steps improved the quality and clarity of the topics generated, making the results more reliable for further exploration. Also, non-ASCII letters (e.g. *TRUSTED*) and bold letters were transformed to standard characters. After preprocessing, chat messages were transformed into bigrams and trigrams to capture contextual relationships and common phrases within the text (X. Wang et al., 2007). To ensure meaningful n-grams, only combinations with strong co-occurrence patterns (threshold of 10) and a minimum frequency of five occurrences were retained. This approach reduced noise and ensured the quality of the data, allowing for a clearer and more interpretable topic analysis. These parameter values were chosen based on manual inspection of the generated n-grams. Furthermore, using the spaCy library, the remaining words were filtered based on Parts-Of-Speech (POS) to retain only those with substantial semantic value, such as nouns, proper nouns, adjectives, verbs, and adverbs (Altinok, 2021). These categories provide critical insights into the content and context of the text, while less informative categories, like pronouns and prepositions, were removed to reduce noise and enhance the efficiency of the LDA model. Extremes were filtered out and the text was then lemmatised, reducing words to their base forms, which significantly decreased the number of unique words and improved data quality (Korenius et al., 2004). The refined text was used to construct a corpus, dictionary, and a bag-of-words representation. Most model parameters were left at their default values, balancing topic and word distribution smoothness (K. Du, 2022). The default *chunksize* and a fixed random state ensured efficient computation and reproducibility. Parameters such as the number of passes and iterations, initially set to their defaults, were later optimised via a grid search to improve model performance, aiming to balance runtime and output quality, while ensuring effective topic-word assignments.

In this unsupervised LDA model, the number of latent topics must be specified as input. To determine the optimal number of topics, the model was run using various ranges. The evaluation focused on coherence scores, interpretability, and topic detail. Coherence scores measure the semantic consistency of words within topics, with higher scores reflecting better topic quality (Röder et al., 2015). Using the elbow method, coherence scores were plotted to identify the point where marginal improvements levelled off (Gurdiel et al., 2021). It is important to recognise that a universally accepted coherence score does not exist, and the interpretation of topics can be challenging for humans (Chang et al., 2009). Instead, the coherence score must be interpreted in combination with the actual content of the topics and the objectives of this analysis. In this study, coherence scores served as an initial guide to narrow down the range of topics, but the final selection was based on a thorough and time-intensive manual review to ensure that the topics were both meaningful and relevant within the context of understanding distinct topics in chat and bot messages. This process involved multiple iterations, focusing on local maxima in coherence scores while ensuring that the topics remained interpretable and aligned with the study's goals. To verify the quality and coherence of the topics, a manual inspection was conducted by exporting 100 full messages per topic, carefully reading and assessing each message to determine whether it aligned with the identified topic. Manual inspection to ensure that the topics were meaningful was done by exporting 100 full messages per topic. Word clouds (see Appendix E) were further used to display how well labels represent the essence of the topic compared to other words within the same latent topic. Other metrics, such as the perplexity score, can also be used, however, perplexity is less intuitive than the coherence score (Gurdiel et al., 2021).

Chat Messages

The model is trained using the remaining 5,488 unique tokens from 66,697 chat messages, with the hyper-tuned parameters *passes* and *iterations* respectively set to 10 and 250. To be able to see whether the current dataset

shows signs of newly formed latent topics, the same approach has been utilised on the reference dataset from Schrama et al. (2022), however, each model was optimised separately. Appendix E.3 presents the full results of this analysis. The significant difference in the number of unique tokens and the number of chat messages of both datasets reveals that the current dataset has limited vocabulary (5,488 versus 53,307 unique tokens) and significantly fewer chat messages to train on (66,697 versus 557,301 chat messages). Therefore, the model based on the current data has limited diversity and leads to overfitting of topics and a lower overall accuracy. The LDA model with chat messages was initially run with 10 to 25 latent topics, but coherence scores were low and declined with more topics, indicating fewer meaningful topics in the dataset. The model was refined to a range of 0 to 15 topics, significantly improving interpretability. This adjustment aligns with the nature of Telegram chat messages, which are typically less detailed and varied compared to forum posts.

Figure 5 shows both the coherence overview plots of the chat messages (on the left side) and the plot for the bot messages (on the right side), which will be used in the paragraph below. As indicated earlier, it is not feasible to draw a conclusion regarding the suitability of the model solely based on the coherence score, which has become evident in the context of the chat messages. The coherence scores for the chat messages highlight that the model performs less effectively compared to similar studies, primarily due to overfitting because of the lower diversity in vocabulary. This may result in certain topics not being highlighted, despite their presence in the data, due to underfitting. From the coherence plot, the three local maxima, featuring 5, 10, and 13 topics, were identified as the most theoretically effective models. An examination was conducted to determine which topics emerged from these three models and how they related to the objective of the analysis, specifically to provide clarification on the discussion points within the chat messages. Ultimately, it was found that the model with 10 latent topics was the best-performing option. Still, some topic groupings contained messages with limited resemblance to each other. Despite efforts to optimise the model through parameter tuning or by adjusting the strictness of preprocessing, further improvements in topic coherence could not be achieved. For the remainder of this study, this means that some topics might seem more important than they actually are, while other less common but still important latent topics might be missed. Also, since some topic groups contain messages that don't have much in common, it can be harder to interpret the results. Human judgement is thereby more necessary than solely relying on the data.

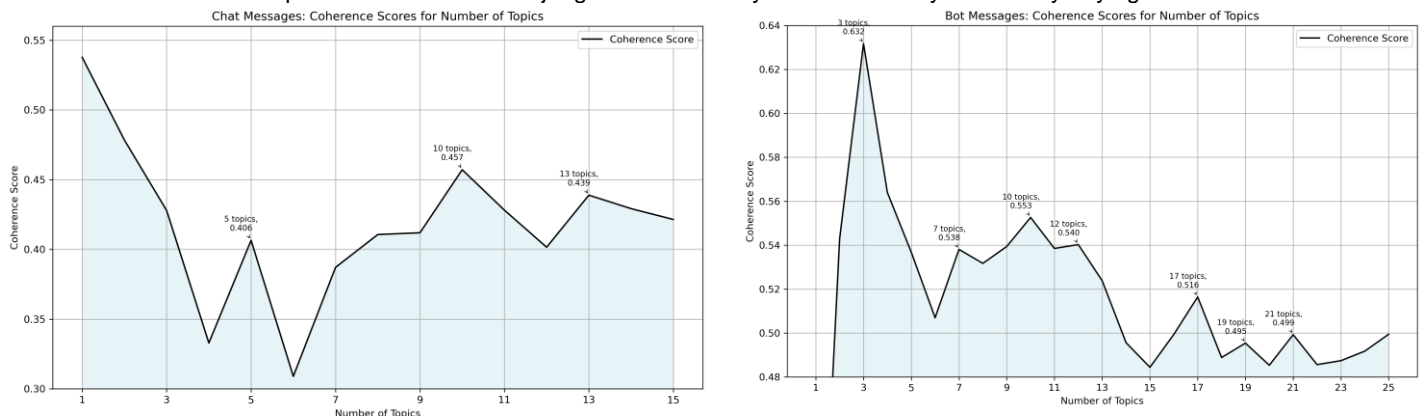


Figure 5: Coherence Scores for Chat Messages (left) and Bot Messages (right)

Bot Messages

To analyse the role of bot messages within Telegram channels, a similar approach as the chat messages was applied to 135,729 bot messages using the same optimisation metrics as for chat messages. A grid search was conducted to refine the model, with the number of passes set to 25 and iterations to 100. One challenge in this analysis was that bot messages frequently included usernames of addressed individuals, leading to a dataset cluttered with non-informative terms that did not contribute to identifying message topics. To improve model performance, strict preprocessing was applied to remove these elements, resulting in a final set of 135,727 bot messages with only 332 unique tokens. This indicates that bot messages rely on a highly repetitive and limited vocabulary, with low diversity and a frequent recurrence of standard words.

Since the number of latent topics was difficult to predict upfront, the model was run for a range of 1 to 25 topics. At first glance of Figure 5 (right), the model with 3 latent topics appears to perform best based on coherence scores alone. However, when the messages were exported that were grouped together by this model, it became evident that topics with little conceptual overlap were combined, leading to a loss of important topics and thereby nuance. While the coherence score for this model is substantially higher than for models with other defined numbers of latent topics, the decision was made to look further. The models with 7, 10 and 12 models provided a more accurate representation of the underlying thematic structure within the dataset. It was found that the model with 12 topics splitted similar subjects over multiple topics, which is not beneficial for the analysis. The model with 7 topics, similar to the model with 3 latent topics, missed (minor) differences in the overarching topics behind the bot messages. Therefore, it was found that the model with 10 latent topics, with 0.553 as coherence score, performed best.

6.4 Finding Payment Methods: Automated Message Indexing

Via automated advertisement message indexing, the correlation between ad category and payment method can further be explored. This provides the possibility to understand if vendors offering multiple categories of crime are more likely to diversify their payment options, compared to single-category vendors. An approach similar to that of Schrama et al. (2022) was therefore applied. This approach has proven effective and relatively easy to implement. The input consisted of raw lowercase labelled messages filtered to retain only advertisements offering products or services. To identify payment methods in the messages, a predefined list of indicative words (*'betalen', 'betaling', 'geld', 'prijis', '✓', 'euro', 'verzonden', 'verzenden' and 'bedrag'*) from the earlier research was utilised. These words are commonly found near terms that specify payment methods. Through manual inspection using Telegram's search function, the accuracy of this list was evaluated. Additionally, an analysis was conducted to detect any payment-related terms that did not appear near the indicative words. The assumption is that as more indicative words are added, the number of missed payment-related terms should decrease. When this number stabilises and no longer decreases, it suggests that the list of indicative words has reached saturation and is sufficient for the analysis. This assumption holds true, as shown in Figure 22 in Appendix F.1.

The list of payment methods (Table 8 in Appendix F.1) has been adapted and expanded compared to previous research. Based on observations, common additional payment preferences were identified. Payment identification terms such as 'PSC' and 'BTC' were added. Additionally, it was noted that forum users frequently use the term 'Crypto' to refer to their payment method, likely referring to Bitcoin. Interestingly, other types of cryptocurrencies appear to be rarely or never mentioned as payment methods in these contexts. Manual analysis has also shown that sellers of illegal advertisements generally only use one term within a payment category. For instance, they will choose either 'cash' or 'contant' in a single message, rather than using both. It was thereby concluded that adding additional payment indication words ('crypto,' 'psc,' 'transfer,' and 'contant') successfully identified more advertisements that would otherwise have been overlooked.

Manual inspection of the messages with a payment method was performed to guarantee that the model only selects payment identification words where they actually specify a payment method. In this process, it was found that words like 'crypto' or 'Tikkie' are often used to refer to (cybercrime) 'panels'. Therefore, the existing blacklist ('panel', 'methode', 'schetsers', 'paneel') was kept, which filters out messages that contain any word from the blacklist, as this might otherwise skew the results. By examining 15 words before and after each signal word, mentions of payment methods were identified, counted, and aggregated by crime type. It was also tried to decrease the number from 15 to 5 or 10, but the model did not accurately capture all messages sufficiently.

Ultimately, among all offer advertisements, 4,210 advertisements were identified in the current dataset where sellers explicitly stated a payment preference within the 15-word range around an indication word. These findings were then plotted for further analysis, enabling the creation of a correlation table between crime types and preferred payment methods. To investigate whether there are empirical differences in these preferences, the analysis is run twice, both on the current and reference dataset. All results, including the insights that can directly be derived from the results, are presented in Appendix F.2 and F.3.

7 Operational Trends & Patterns

In the previous chapter, the specific technical approaches employed for all analyses were outlined. Throughout the analyses, several insights already came forward, such as channel and message descriptives, the occurrence of certain types of messages and the categories of crime offered, and the number of unique messages in the dataset. Besides these insights, several overarching themes and patterns in the increased level of professionalisation of vendors and Telegram as a market can be derived, which will be explained in this chapter, while being underpinned with actual observations within the dataset. These themes are structured into four topics and associated subchapters. Subchapter 7.1 explores the professionalisation of individuals and Telegram as a market, by presenting the frequent use of bots and automation for auto-deletion, message and channel marketing and distribution, and channel moderation. Subchapter 7.2 dives deeper into content distribution, by examining the number of views and shares that messages have accumulated, showing the possibility of rapid message spreading across multiple channels with minimal effort. Subchapter 7.3 presents indications of large-scale channel closure and mechanisms that nevertheless provide methods for the resilience of Telegram as a market. Chapter 7.4 examines the specialisation and diversification in channels and under vendors. By analysing their product range and payment preferences, insights about their professionalisation and channel disruption can be derived.

Besides the aforementioned topic-specific insights, several general observations can be made based on channel and message descriptives. Appendix B provides a comprehensive descriptive overview of the channels, including information about creation and closure dates, the number of messages, the number of unique message authors, information on whether the channel is still online in early February 2025 and the number of subscribers or members of a channel. The channels *General_16*, *General_15*, and *General_24* represent the largest channels within the dataset, although they are not necessarily the longest-running channels. Furthermore, there are several channels, such as *General_6*, *General_14*, and *Fireworks_2*, that, despite their extended duration, have a relatively low volume of messages. Further analyses partly draw on the found insights from this appendix.

7.1 Automation and Self-Regulation

The first overarching insight can be found in the field of automation and the frequent use of bots in illicit channels. Subchapter 7.1.1 presents findings on the widespread use of the auto-deletion function within channels and its impact on the researched data. Subchapter 7.1.2 explores the commoditisation of Telegram-related services, such as outsourced message distribution of offer advertisements by third parties. Last, subchapter 7.1.3 examines the use of bots for channel moderation, which facilitates mutual trust within channels and aims to prevent access by lurkers and law enforcement agencies.

7.1.1 Message Auto-Deletion

First, it is observed that several major channels have implemented an automatic expiration date for messages, typically set to one or two weeks. This mechanism results in the automatic deletion of older messages. In the channel *Local_1*, this is particularly evident. Here, older messages are visible within the channel. At a certain point, a bot message appears: '*Pietje set messages to auto-delete in 1 Week*', after which only the most recent messages from the past week are now visible. This trend is also clearly reflected in the current count of scraped messages over time, as illustrated in Figure 6. Since most of the messages now come from the last two weeks of the dataset, it becomes challenging to understand trends within the currently scraped timeframe, as there is simply too little data available over the years. As a result, when conclusions must be drawn about the adaptive behaviours of communities over time throughout this chapter, this must be done by building upon the reference dataset.

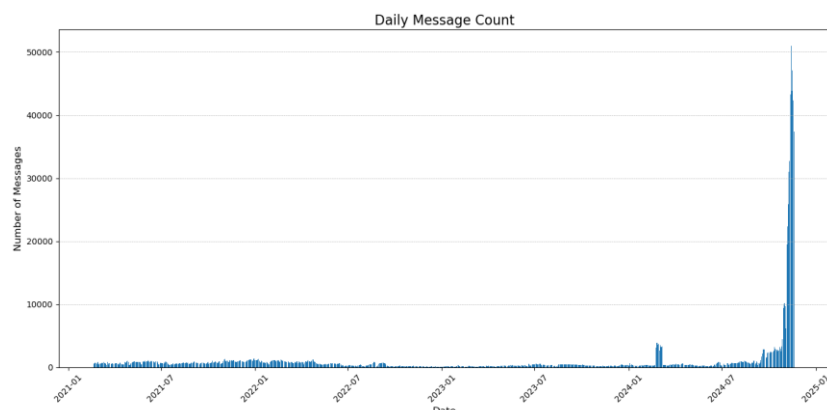


Figure 6: Message Distribution over Time

7.1.2 Commoditisation of Message Distribution

The message in Figure 14 (Appendix C) highlights a second emerging trend: the outsourcing and commoditisation of automated message distribution by intermediaries. Many channels feature messages from intermediaries offering their services, often for a fee, to manage the automated sending of messages on behalf of others or to advertise for channels in other channels via subscription models. This outsourcing trend aims to grow channels and the sales of products on behalf of clients via APIs, being able to reach hundreds of channels simultaneously. Besides automated distribution, individuals offer courses or sell guides that teach others how to engage in fraudulent activities, such as swiping or bonking (techniques where orders are placed on e-commerce websites without completing payment). Rather than merely offering or using products and services themselves, vendors are actively trading knowledge and commoditising expertise in the form of courses and instructional materials.

Due to the widespread use of message distribution services, many identical messages were found in the dataset. Table 6 in Chapter 6.2 presents the number of unique messages identified, categorised by message type across the two datasets. These insights are visualised in Figure 7 and form the basis for several empirical observations regarding changes on community level and the general use of Telegram as an illicit market. Firstly, request advertisements and chat messages show a relatively high number of unique messages, which is expected since these messages are typically tailored and not automatically copied and pasted across multiple channels. In contrast, there are fewer unique messages among bot messages and offer advertisements, indicating the large-scale use of automation to forward messages. Advertisements are essentially broadcasted across channels in a ‘shotgun’ approach. The most frequently identical message was sent 25,012 times and pertains to the sale of anabolic steroids (see Figure 13 in Appendix C). Additionally, the substantial decrease in the number of bot messages suggests that bots are now used more selectively compared to the period between 2017 and 2021. Overall, these findings suggest that Telegram has increasingly functioned as a broad marketplace with generic advertisements, rather than as a chat environment. In total, unique messages account for only 5.3% of the dataset, compared to 21.8% previously, highlighting the high frequency of repetitive messages, especially in offer advertisements.

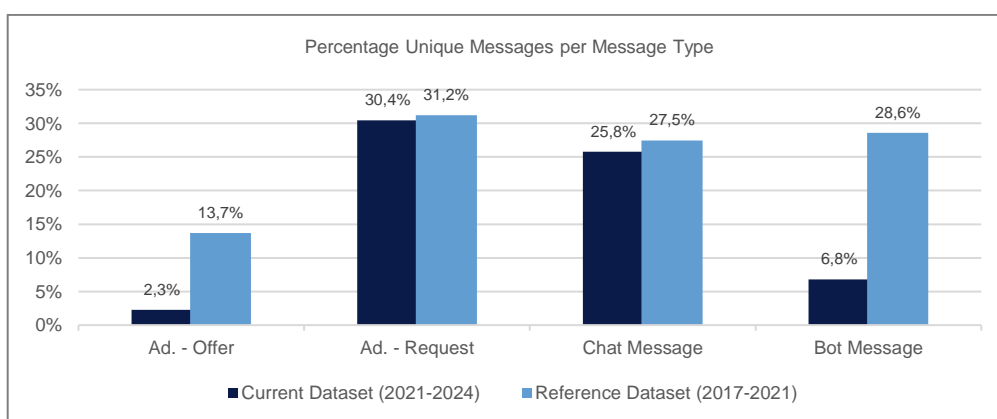


Figure 7: Unique Messages per Message Type

Bots have significantly simplified the process of sending (automated) offer advertisements. This low level of uniqueness in the variation of messages has serious consequences on the advertisements that members of illicit Telegram channels face. Figure 8 provides an overview of the total number of offer advertisements per user (represented in blue). Notably, many users have sent over 100 advertisements within the scraped timeframe. Specifically, 321 users have sent between 1,000 and 5,000 messages, and 16 users have sent more than 5,000 messages. However, these numbers are skewed due to this widespread use of bots. To address this, the analysis also examines the number of unique messages sent per account, shown in orange, determined by identifying identical message texts. Messages with minor adjustments, such as additional emojis or formatting changes, were not classified as duplicates. The results reveal that the number of unique messages is significantly lower, with only 7 authors sending between 100 and 500 unique messages. In certain channels, this leads to a significant reduction in the number of messages. For instance, *Cashout_3* contains 1,062 messages, of which only 42 are unique.

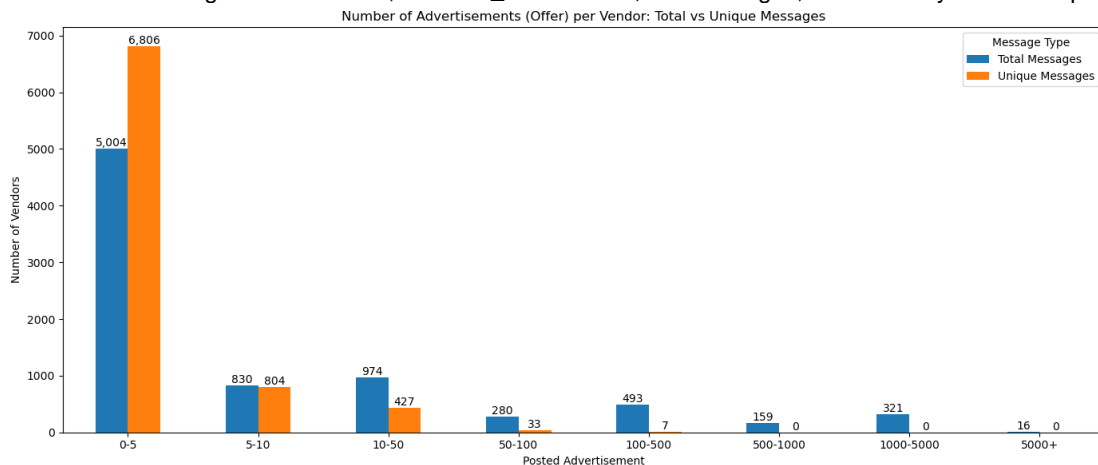


Figure 8: Total and Unique (Offer) Advertisement Sent per Vendor

In addition to the extensive use of bots for message forwarding, sellers have adopted another clever tactic from the advertising and marketing field. This is the inclusion of SEO (Search Engine Optimisation) tags at the bottom of messages, as can be seen in Figure 14 in Appendix C. Vendors add frequently searched keywords to increase the likelihood of their messages being discovered when users utilise Telegram's search functionality or the search feature within channels to find specific products or services. This technique, borrowed from major search engines like Google, further shows how vendors use professional strategies to improve their visibility and attract more attention to their offerings.

7.1.3 Channel Moderation



Besides the automated distribution of messages and the automatic deletion of messages after a set period, bots are several other moderation and governance mechanisms, namely functioning as gatekeeping mechanisms, detecting scammers and bringing up trust, maintaining order by warning and banning users and welcoming users. The first notable used tactic involves restricting access to certain channels by requiring potential new members to complete specific tasks, functioning as a gatekeeping system. For example, bots send a specific user an automated message with an invitation link, that has to be forwarded to other channels or contacts multiple times, before one is granted access. This approach, illustrated in Figure 9, serves multiple purposes: it deters lurkers, promotes the channel through widespread link sharing, and creates a sense of privacy. In these prompts, users are directly linked to associated broadcasting channels, where a list can be found of trusted channels, creating a network of allied vendors and a further sense of marketing of channels. This will be further elaborated in chapter 7.3.



Figure 9: 'Share to Unlock' and 'Join All Channels'

The prevalence of the use of bots to control access to Telegram channels is further affirmed by the LDA analysis of chat messages. Hereby, in the fourth found topic, conversations are revealed in which members are encouraged to join other channels, including those offering other types of criminal activities. Examples include online casinos, (sports) gambling and carding techniques. Discrete and exclusive access is thereby often mentioned in the chat messages, including invitation URLs that allow users to join a channel with a single click.

Second, bots are used for scammer detection and trust verification. This was found in the topic modelling analysis with bot messages, combining latent topics 1, 8 and 10. Automated warnings, where users are notified for specific (scamming) users, are used to warn users against fraudulent sellers, besides the use of blacklists and scam registers (e.g. 'trustregister' or 'Oplichterspotje'). Users of groups are directed to other channels for these blacklists and registers, where banned user lists can be found. The use of such bots shows the self-regulating nature of these communities, where members attempt to protect themselves from scams while still engaging in illicit trade.

Third, bots are used for channel governance, such as informing users about channel guidelines and functioning as spam control, which was found by combining latent topics 2, 3, 4, 5 and 6 within the bot messages. Bots are thereby used for automated moderation to maintain order, by enforcing channel guidelines by muting, banning, and kicking users for violations such as excessive messaging ('### has been kicked for sending messages that are too long'), unauthorised link sharing ('### has sent a  Link without authorisation. Action: Muted  until 08/09/2024 20:38'), and suspected spamming. To block spammers, some administrators use self-made and shared lists, however, one often-adopted system stands out. Many messages about spammers are sent by 'Combot', which is part of an external anti-spam API (Combot Anti-Spam System, abbreviated as CAS), which can be used both through free and paid options. This is a system that operates independently of channel administrators and functions entirely autonomously. Once users are flagged as spammers, they can no longer join channels that are part of the CAS network (Combot Anti-Spam System, n.d.). An example of such a message is: '### has been banned! Reason: CAS ban' or 'Waarschuwing! ### is een bekende spammer en is geblokkeerd door CAS. Combot raadt aan deze gebruiker te blokkeren.' (translation: 'Warning! ### is a known spammer and has been blocked by CAS. Combot recommends blocking this user'). These automated policing mechanisms reveal an attempt to maintain a functional trading environment while minimising unwanted disruptions, thereby using legitimate software being used illegally. In channels where the use of bots is less prevalent, individual users assume a similar role by alerting one another. From the chat messages, two topics (numbers 8 and 10) were found that discuss fraud prevention and scam awareness. Criminals warn each other about other users within channels, for example, if they have been scammed themselves or know of someone else who has been scammed. This includes vendors and buyers who fail to show up, charge unfair prices, or provide low-quality products. These individuals are tagged to identify them for others.

Last, bots are used to guide users to new channels and to welcome them when joining a new channel ('### welkom in de handel groep van NL/BE, succes met de verkoop!!') (translation: 'Welcome to the NL/BE trade group, good luck with the sale.') This topic shows close resemblance to the second found latent topic from the reference dataset (see Appendix E.3), including the often-mentioned URLs to new channels. Users are redirected to overview pages or broadcasting channels, where complete lists with (new) channel names can be found.

During the manual inspection of bot messages, a forwarding channel was found that had attracted more than 110,000 subscribers. In this channel, various bots were offered that automatically moderate Telegram channels by removing specific types of messages such as cryptocurrency addresses, URLs, and commands from non-admin users. They can also warn about potential sleeper or scam accounts that have no username. By filtering out spam, suspicious links, and certain keywords, they help keep channels more organised and can reduce the visibility of scam attempts. It is therefore possible that messages which have been sent without permission, or did not follow the channels' guidelines, are removed before other participants view that message.

7.2 Views, Shares & Contributors

This section explores how the platform's forwarding mechanisms, channel dynamics, and message visibility (such as message views and shares) contribute to the fast amplification and distribution of illicit content. Appendix B has provided insight into the number of members or subscribers and the number of contributors of a channel, as of December 6, 2024. The number of contributors varies significantly, ranging from a few individuals to thousands in certain channels. While this may seem minimal, an examination of their reach, indicated by the number of members or subscribers, reveals that they do indeed have considerable influence. It is important to make two side notes with this parameter. First, the number of members of a channel does not provide a complete picture. For instance, individuals can view a channel and privately respond to advertisements or messages without being a member ('lurking' or 'creeping'). Consequently, the actual reach is much broader than what is reflected on paper. It was observed how easily one can browse through channels based on keywords, without being a member of the channel. However, it is reasonable to anticipate that users within the examined channels engage across multiple channels simultaneously, rather than exclusively offering or requesting products or services through a single channel. Based on the available data, it is not feasible to make definitive further statements regarding this matter.

From these insights, various conclusions can be drawn. Channels with many members but only active for a short time show that these channels can quickly attract people when needed. This can be achieved by the implementation of the earlier mentioned gatekeeping system, where a new member is required to forward the invitation link to several other chats before they are permitted to join the channel. This can happen in situations where there's urgency or high demand for specific goods or services. Fast disappearance can be allocated to either voluntary shutdowns to avoid detection, or when Telegram or law enforcement take a channel offline. Channels with short lifespans and high member counts reflect how criminals adapt to pressure, by shutting down and starting new channels quickly, helping them to stay active while reducing the risk of being caught. On the other hand, channels that stay active for a long time but have fewer members might be focused on more niche or specialised purposes. Overall, there appears to be no direct correlation visible between the lifespan of a channel and its member count, indicating that factors such as content type, promotion methods, and reputation are more important for a channel's success and reach.

Additionally, it is interesting to understand how often sent messages are being viewed and shared. The range of the number of views and shares per message varies substantially, as displayed in Figure 10. The upper boxplot displays the accumulated views of individual messages. The lower boxplot shows the combined distribution of message shares. In both boxplots, the orange marker demarcates the median. When analysing the number of views, it is noticed that the distribution shows little resemblance to a normal distribution, but is heavily skewed with some posts with more than 120,000 views. The most-read message in the current dataset has been viewed 841,740 times, showing the enormous reach that a message can exert. However, this metric accounts for all views across the channels where the message has been forwarded, meaning it was not viewed this often within a single channel. Despite this, the metric underscores the significant scale and visibility of certain messages. It is essential to note that the most viewed messages within the dataset are all classified as 'Ad. – Offer' and 'Cybercrime'. These messages offer (loaded) PayPal accounts, tutorials on how to use them, and simulated crypto payments (for fraudulent purposes). The top-3 messages have attracted more than 600.000 views each, and are all in English, indicating significant international influences in Dutch Telegram channels.

When the number of message shares is analysed, a skewed distribution is observed too. With a median of 3238, it is evident that numerous messages are being widely forwarded across multiple channels. Many identical messages are now frequently circulated, making them less tailored to individual channels. The most forwarded message (shared 133,096 times) was viewed 151,282 times. The most shared messages, similar to the messages with the most views, are all written in English and promote fraudulent payment platforms and services on a massive scale, showing international involvement in Dutch Telegram channels. Regarding these numbers, an important side note needs to be made. These numbers were not downloaded for all messages during the scraping process. Initially, it

was suspected that this issue was related to the Telethon API, but it was later discovered that it was determined by the type of message being scraped. Specifically, only messages forwarded from a broadcasting channel or messages originally sent within such a channel include the views and shares parameters (Lonami, 2021).

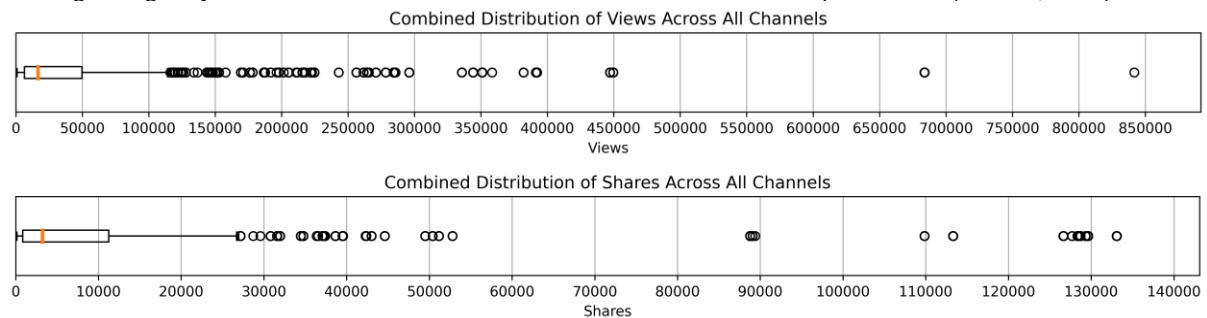


Figure 10: Message Views (upper) and Shares (lower) Boxplot

Based on these insights, the impact of message forwarding can be derived. The high view count does not necessarily indicate that a single channel has a vast audience, as many messages have more views than there are subscribers in a channel; rather, it reflects the cumulative views across multiple forwarded locations. In combination with the high number of times that messages have been forwarded, shows that Telegram's forwarding mechanism acts as a multiplier for illicit content.

7.3 Channel (In)continuation

The channels that were scraped provide insights into the adaptive behaviours of Telegram communities; however, as noted in Chapter 6.1, several channels were taken offline either during the scraping process or throughout the analysis. Between September and early November 2024, 26 market channels either ceased operations or were made private. Among these 26 closed channels, 12 were general channels, 5 were drug-related, 1 focused on local trade, 6 facilitated cashout operations, 1 dealt in firearms, and 1 specialised in fireworks. In addition to the channels that could not be scraped, seven other markets were shut down completely during the writing of this report. Hereby, six channels did not disclose their reason for closure, one channel displayed: *'This channel can't be displayed because it violated Telegram's Terms of Service'*, and one channel was temporarily suspended by Telegram: *'This group has been temporarily suspended to give its moderators time to clean up after users who posted illegal pornographic content. We will reopen the group as soon as it complies with the Telegram Terms of Service again'*. The seven markets that completely ceased operation focused on weapons (1), local activities (1), cash-out (1) and general offerings (4). In conclusion, of the 71 identified channels that fulfilled the set criteria of this research, only 38 were still active in early February 2025.

This indicates two key points. Firstly, we are informed by a specially created website that Telegram has begun to actively monitor and moderate channels (Telegram, n.d.-a). Based on the observations mentioned above, we can assert that this targets included channels from this study, and that administrators and vendors face increased risks within these channels. While a direct causal link between channel closure and the increased cooperation between Telegram and authorities cannot be empirically confirmed, the timing and the increased of auto-delete, suggest a deterrence effect. Besides, the topic modelling analysis of chat messages has empirically revealed that there are no explicit discussions regarding a mass exit to other platforms or more private types of conversation.

Even though channels are being removed from the platform, it has been observed that channels can attract a significant number of members or subscribers in a short period. Various channels with limited consecutive activity when their lifespan was analysed, such as *Local_5* and *General_4*, have attracted many members. Although no further messages are being sent, individuals can still join a channel and view previously sent messages (given that they have not been removed). This facilitates the continuation of exchange, even in the absence of recent activity. Furthermore, there are alternative methods through which activity in a (new) channel can be rapidly restored. First, from the analyses of the number of views and shares, it is known whether a message was sent manually, or whether

it was sent and forwarded through a broadcasting channel (or if the channel itself operated as a broadcasting channel, where only administrators can send messages). By examining the percentage of total messages with a recorded view count, it is possible to determine the proportion of messages forwarded from other channels. This tells something about the extent of adaptability of vendors. Appendix B therefore includes a column titled '% Broadcast', which indicates the percentage of messages in a channel that are forwarded. The variation in these percentages is substantial. For instance, 15 groups have over 90% of their messages forwarded from other channels or operate solely as broadcast channels. For example, in *General_1* (94.9% broadcast), most messages are sent exclusively by administrators, suggesting a one-way communication strategy with minimal user participation. These channels likely function as announcement boards. In *Cashout_1* (100%), over a span of 181 consecutive days, a single individual sent only 28 messages but managed to attract 925 followers. This demonstrates the significant influence a single user can yield. The messages in this channel are therefore also more likely to appear on a large scale in other channels. Thus, broadcasting channels increasingly act as resilient distribution hubs, that function as one-way announcement boards with high forwarding activity. Even when primary transaction channels are taken offline, these broadcast channels can quickly redirect users. When channels are not taken offline but there is no recent activity, they still facilitate crime by functioning as static repositories.

Furthermore, the aforementioned gatekeeping system and the automatic deletion function contribute to the discovery of new channels by the relevant target audiences, and they eliminate the possibility of reviewing past activities of channels or vendors. The gatekeeping system, in particular, facilitates (internal) crime displacement, as it enables criminals to swiftly switch channels to avoid detection, or when channels are held offline.

7.4 Channel and Vendor Specialisation

This section examines the levels of specialisation, professionalisation and diversification of illicit vendors, by analysing their product range and payment preferences. Besides, by investigating the relationship between supply and demand across different crime categories, insights about market dynamics, scarcity-driven demand, and how criminal actors adapt to enforcement actions and platform disruptions, can be derived. First, in Figure 4 (Chapter 6.2), the distribution of found crime categories per channel has been presented. From this figure, it becomes evident that while some channels are highly specialised, the majority are broader in scope than their names suggest. Channels specialising in the sale of fireworks, firearms and explosives tend to focus almost exclusively on these categories. In contrast, other groups presenting themselves as dedicated marketplaces for drugs, cash-out services, or cybercrime often feature a mix, offering mixed illicit goods and services interchangeably.

By narrowing down to the level of individual vendors, it can be investigated how many different categories a vendor offers, as this can indicate whether they specialise in a single product or offer a range of products. To explore this, a distribution was plotted showing the number of unique advertisement categories linked to each Author ID. A vendor with only one unique category is classified as a single-category vendor, while those offering multiple categories are considered multi-category vendors. Figure 11 illustrates this distribution, revealing that 67.6% of vendors fall into the single-category group, while the remaining 32.4% are multi-category vendors.

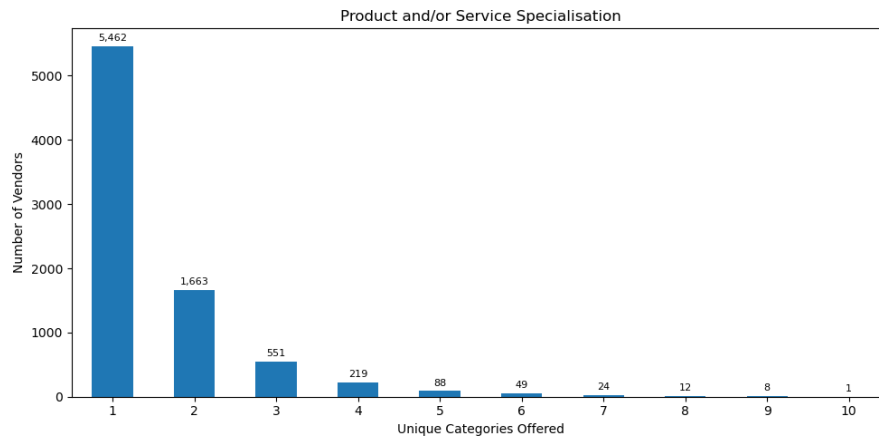


Figure 11: Product Range Specialisation

At the same time, it is known which payment preferences are stated by vendors. The detailed approach for this analysis has been presented in chapter 6.4, and all results can be found in Appendix F. By understanding whether single-category and multi-category employ different strategies for payment acceptance, further insights about specialisation and professionalisation under vendors can be derived. Appendix F.2 has examined the relationship between crime categories and payment methods, but this does not address the decision-making of multi-category vendors. In Appendix F.3, it is found that, among vendors specifying a payment method, single-category vendors accept an average of 1.37 payment methods, while multi-category vendors accept an average of 1.63 payment methods throughout their advertisements. This difference is statistically significant, so, multi-category vendors accept a wider range of payment methods compared to single-category vendors due to their diversification of product offerings. The exact distribution of accepted payment methods, both for single-category and multi-category vendors, is displayed in Figure 26 in Appendix F.3.

In general, shifts within the Telegram communities regarding payment preferences can be witnessed. Drug- and pharmaceutical-related transactions have shown a strong shift towards cash in recent years, likely due to the physical nature of these exchanges and pre-existing in-person networks. Meanwhile, bank transfers and 'Tikkie' have declined, except in hard drug sales, as criminals prefer anonymous methods like Paysafecard to avoid traceability. Cybercrime and cash-out operations heavily depend on PayPal, Paysafecard, and cryptocurrencies due to their pseudo-anonymity and ease of online use. Cash also plays a role in financial crime, particularly for counterfeit money exchanges, where fake currency is traded for real cash. These shifts reflect increasing concerns about anonymity and law enforcement detection.

Where earlier analyses have mainly concentrated on offer advertisements, it is interesting to turn this around and examine the interaction between supply and demand for all crime categories. This leads to an understanding of which categories experience relatively higher demand and where individuals are explicitly seeking products. If groups that offer these products are removed from offline platforms, it may also result in an increase in demand. Figure 12 illustrates the distribution between offers and requests across categories. The data shows that for drugs, pharmaceuticals, cybercrime, and documents, nearly all advertisements are offer-based. Conversely, (fire)weapons, fireworks, cashout, stolen goods, and 'other' categories have a relatively higher proportion of request-based ads, which aligns with expectations, and requires individuals more effort to obtain. The lower volume of advertisements in these latter categories likely means that such posts appear less frequently in user feeds, prompting individuals to request specific products or services, showing scarcity-driven demand among Telegram users. If Telegram or law enforcement disrupts channels specialising in high-demand categories, users shift towards request-based interactions to compensate for the loss of supply.

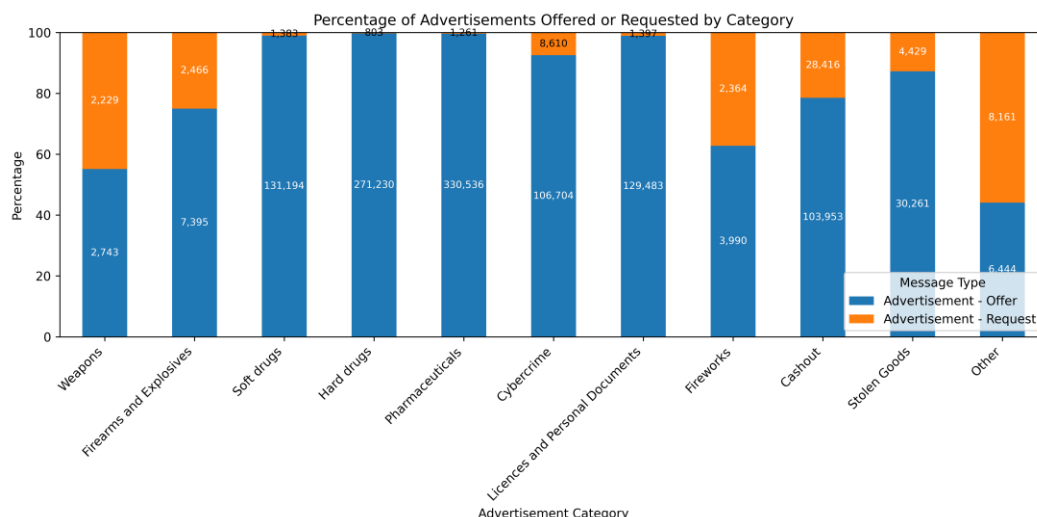


Figure 12: Offer and Request Distribution per Category

7.5 Conclusions

The Telegram data from 2021 to 2024 reveals several intriguing and novel insights, which can be categorised into four main themes. The first observed theme focuses on how criminal actors utilise Telegram's built-in technological capabilities for automation, self-regulation, and commoditisation. Bots and automated systems play a crucial role in governing channels, managing membership, and improving security, transforming Telegram into a structured yet adaptive marketplace. A key mechanism in this process is message auto-deletion, where channels automatically erase older messages after a short period. This reduces exposure to law enforcement and minimises the visibility of past advertisements, creating a sense of privacy and security. Additionally, distribution bots automate message forwarding across multiple groups, ensuring the widespread and rapid spreading of illicit advertisements. Another observed trend is the outsourcing of Telegram-based services. Intermediaries offer paid marketing and automated message distribution across numerous channels using API-driven bulk messaging. Similarly, fraud-related knowledge is commoditised, with vendors selling guides and courses on illegal activities such as 'bonking'. Access to certain groups is also controlled through gatekeeping bots, which require new members to complete promotional tasks, such as sharing invitation links in multiple groups, before they are granted access. Despite the illicit nature of these groups, self-regulation is actively maintained to ensure order and reduce fraud within the community. Bots function as scam detection tools, automatically identifying and warning users about fraudulent vendors by referencing shared blacklists. Additionally, anti-spam systems enforce channel guidelines by banning spammers, often operating autonomously to block flagged accounts across multiple channels. Many of these automated techniques were originally designed for legitimate purposes but have been repurposed for unlawful activities. Bots intended for community management are exploited for law enforcement evasion, scam prevention, and membership control, showing the adaptability of illicit networks to digital enforcement measures. In channels where bots are not used, manually written chat messages by users are sent to warn others to warn and protect others.

The extensive use of distribution bots is also highlighted in the second observation, which builds on the number of views, message shares, and contributors. The findings indicate that messages within illicit Telegram channels are increasingly generic and not tailored to specific audiences. This has resulted in a significant decrease in unique messages, particularly among offer advertisements. Rather than making advertisements tailored to specific channels or audiences, vendors rely on mass-distributed, pre-written advertisements, creating a more standardised and impersonal exchange. The data reveals that only 5.3% of messages in the dataset are unique, compared to 21.8% in the reference dataset, emphasising the shift towards automation for offer advertisements and bots. This trend thereby highlights Telegram's transformation from a chat-based forum into a large-scale illicit marketplace. Instead of stimulating interactive discussions, channels primarily serve as digital billboards where the same advertisements are repeatedly forwarded simultaneously across channels. The platform's forwarding mechanisms

further amplify the reach of these messages, with some receiving hundreds of thousands of views and shares. The most widely circulated messages, often written in English, indicate international involvement in Dutch channels.

Third, the data suggests that Telegram is increasingly cooperating with authorities to monitor and moderate illicit channels. This is reflected in the removal of dozens of market channels during the research period, as well as the temporary suspension of two channels for violating Telegram's terms of service. While a direct causal link between channel closure and the increased cooperation efforts between Telegram and authorities cannot be empirically made, the timing of these closures, alongside the increased use of auto-deletion features, suggests a growing deterrence effect. Channel administrators and vendors appear to be aware of these risks, leading to more strategic use of security measures, such as restricted access and auto-deletion. Despite these enforcement efforts, no evidence was found of a mass migration to alternative platforms. The topic models of chat and bot messages revealed no widespread discussions about moving to other services, indicating that Telegram remains a key platform for illicit activities. Instead, vendors and groups demonstrate adaptability by using broadcasting channels to maintain visibility and distribute messages widely, even after individual channels are removed. The ease of creating new channels and swiftly attracting new members facilitates dynamic displacement in Telegram itself. The cycle of opening a channel, drawing in subscribers, and then shutting it down demonstrates why combatting these groups is difficult; merely shutting down a channel does not suffice, as they rapidly rebuild elsewhere. Additionally, inactive channels, where messages can still be found but are no longer used for active communication, continue to serve as crime repositories, allowing criminal exchanges to persist even without new messages being sent.

In the fourth and last identified trend regarding channel and vendor specialisation, three main observations emerged. First, findings reveal that specialisation within illicit Telegram markets is not primarily observed at the channel level but rather at the level of individual vendors. While some channels appear specialised based on their names, most facilitate a broader range of illicit activities, offering a mix of goods and services. Targeting and removing channels based on specific types of crime is therefore less meaningful, as the various forms of criminal activity are widely dispersed. However, at the vendor level, clear distinctions emerge. The majority (67.6%) of vendors focus on a single category, while a smaller portion (32.4%) engages in multi-category vending, diversifying their offerings across multiple crime types. Second, scarcity-driven demand is observed in the advertisement data. This is evident in categories where supply is limited, leading users to actively request specific goods or services rather than relying on existing offers. This pattern is found in categories where fewer advertisements result in an increased number of request-based messages. A third, last and new key finding is the statistically significant difference in payment preferences between single-category and multi-category vendors. Multi-category vendors accept a wider range of payment methods (1.63 versus 1.37 payment methods on average), likely due to their diversified product offerings, requiring greater flexibility in transactions. This suggests a higher level of professionalisation among these vendors, as they adapt their payment strategies to maximise customer accessibility, minimise risks of detection and show that vendors adjust their methods in response to enforcement actions and market conditions.

To sum up, this chapter has provided empirical evidence of mechanisms that provide capacity for change. Telegram's illicit ecosystem is shaped by automation, self-regulation, and commoditisation, with bots playing a crucial role in governance, security, and content distribution. While these mechanisms enable rapid change and resilience, they reflect more of a structural evolution of the ecosystem rather than individual adaptation. Vendors increasingly rely on standardised, mass-distributed advertisements, shifting Telegram from an interactive chat platform to a large-scale marketplace. Although enforcement efforts have led to channel closures and increased self-imposed security measures, there is no evidence of a mass migration to alternative platforms. Instead, the ecosystem adapts collectively through broadcasting channels, temporary shutdowns, and flexible payment strategies, demonstrating how Telegram evolves as an illicit market.

8 Discussion

This chapter contextualises the quantitative findings from Chapters 6 and 7, through the theoretical lens that has been formed using literature and interviews (Chapters 2, 4 and 5). Implications and scientific contributions are hereby presented in Chapter 8.1. It is hereby highlighted how Telegram has evolved into a heavily commoditised illicit market, relying on automation, internal crime displacement, and specialised vendor strategies. The limitations section (Chapter 8.2) discusses methodological constraints, including data collection challenges, the impact of auto-delete and mass message forwarding, and other issues related to earlier individual analyses. The reflection (Chapter 8.3) explores how the research design shaped the results, and it presents areas for future research. Lastly, recommendations for law enforcement and policy are presented in Chapter 8.4.

8.1 Placing the Trends in Context

This chapter presents the key contributions of this research, providing new insights into the resilience of Telegram as an illicit market, its operational mechanisms, and the broader implications for academic research and society. The findings partly challenge existing assumptions about Telegram's role in criminal ecosystems, demonstrating that it has transformed from a messaging platform into a heavily commoditised marketplace, where automation, self-regulation, and specialised vendor strategies drive market sustainability.

The first contribution (Chapter 8.1.1), highlights how automation has fundamentally altered Telegram's illicit landscape. The widespread use of bots for various purposes has minimised the role of personal interactions, reducing Telegram's function as a communication platform and instead positioning it as a large-scale advertising system for illicit services. This structural change challenges conventional perspectives on cybercrime communities (e.g. dark net markets), where social ties are often seen as central to trust-building and market participation.

The second contribution (Chapter 8.1.2) builds on the theories of crime displacement and multi-homing, showing that illicit actors do not necessarily migrate to other platforms in response to law enforcement pressure. Instead, mechanisms are presented that enable internal shifting, relying on invitation-based gatekeeping and automated cross-listing to maintain visibility and accessibility. Unlike previous studies that focus on displacement across platforms, this study emphasises how Telegram's design facilitates resilience rather than disruption.

The third contribution (Chapter 8.1.3) shows how illicit actors structure their activities within Telegram. Findings reveal that specialisation occurs at the vendor level rather than the channel level. Additionally, the study identifies scarcity-driven demand, where illicit goods with lower supply generate higher proactive user requests. Furthermore, shifts in payment preferences, and the mechanisms driving these, are presented.

8.1.1 Telegram's Transformation from Messaging Service to Heavily Commoditised Market

First, the findings of this research indicate a fundamental shift away from personal interactions within Telegram. The messages in this study have a uniqueness rate of 5.3% (as presented in Table 6 and Figure 8), which is mainly influenced by the low variety in offer advertisements and bot messages. Compared to a uniqueness rate of 21.8% in the reference study (2017-2021), a stark contrast with a sharp decline in tailored, context-specific interactions is observed. The high surplus of duplicate messages is driven by increased automation within the ecosystem. This includes the mass distribution of advertisements through bots, a service that is now heavily commoditised by intermediaries. Additionally, the widespread use of auto-delete functions further reduces message variation. Repurposed messages lacking customisation to the target audience are hereby simply copied and pasted, resulting in Telegram users being frequently flooded with identical advertisements. While earlier studies have suggested that social ties play a crucial role in sustaining illicit communities, the recent reliance on automation in Telegram means that vendors are less dependent on one-on-one relationships and more reliant on broad and decentralised exposure (Chua & Wilson, 2023; Mador, 2021). Rather than negotiating directly with buyers, vendors prioritise visibility and scalability to maximise reach. This represents a structural change in the market itself, where Telegram less functions as an interactive chat environment for demand and supply, but more as a large-scale advertising platform with

minimal organic interaction between buyers and sellers. Due to this different structural understanding and perspective on Telegram communities, this study proposes that similar existing research (e.g. Boersma, 2023; Schrama et al., 2022), and future research could benefit from being approached through a different lens, one that accounts for the high volume of duplicate messages. In a more extensive reflection in Chapter 8.3, considerations for how such studies should be read and conducted in the future are elaborated upon.

Second, this research has found that illicit channels use automation mechanisms to achieve self-regulation, instead of requiring direct user-to-user trust. Literature on dark net markets has emphasised peer-to-peer trust mechanisms, such as escrow services, vendor ratings and administrators enforcing vetting processes, to create trust in environments where formal enforcement is absent (Armona, 2018; Barratt & Aldridge, 2016; Jardine, 2021). In contrast, the Telegram ecosystem lacks these built-in trust mechanisms, but communities can stimulate trust by increasingly automating self-regulation, thereby shifting from individual negotiations to centralised technological solutions at the channel level. Multiple automated systems are thereby deployed. First, channels use large-scale auto-deletion, ensuring minimal retention of evidence and limiting the impact of observation by law enforcement. Second, gatekeeping systems require new members to share invitation links before gaining access, both filtering out lurkers and expanding market visibility. Third, scam registries and bot-driven fraud detection replace traditional user-based reputation systems, creating centralised scam prevention instead of mutual feedback. Finally, external anti-spam APIs and automated moderation act as enforcement tools, banning flagged users and restricting unauthorised content. These findings partly challenge the notion that the channels are unstructured (P.-Y. Du et al., 2018; Hughes et al., 2024). Instead, its structure is emergent and more automated, rather than solely socially or administratively imposed. The reliance on bots and automation mirrors traditional marketplace enforcement but operates more through technological capabilities rather than explicit rules or social hierarchies.

Third, this study demonstrates novel ways in which services are commoditised. Previous research on commoditisation in cybercrime has mostly focused on the sale of hacking tools, stolen data, and financial fraud services. These studies highlight how barriers to entry in cybercrime markets have lowered, allowing even those with no technical skills to participate by purchasing pre-made tools (Kruisbergen et al., 2019; Schrama et al., 2022; Van Wegberg, Tajalizadehkhoob, et al., 2018). This study builds on that concept but reveals a novel trend in Telegram's illicit ecosystem: advertisement services, scam detection, and market visibility have now also become commoditised. Instead of vendors promoting their own ads, vendors pay third parties to distribute messages, boost visibility, and manage marketing campaigns. Automated bulk messaging services allow criminals to flood channels as shown earlier, further shifting Telegram away from social interactions toward a mass-market advertising platform. Another key finding hereby is the commoditisation of knowledge. Rather than only selling the services itself, vendors sell training programmes, guides, and scamming methods at scale. This further removes the need for pre-existing knowledge or insider connections as new criminals can simply buy instructions on how to commit crimes (mostly fraud). While prior research has examined automated cybercrime services, this study is among the first to demonstrate how Telegram itself has transitioned into a predominantly automated marketplace, significantly reducing reliance on direct user interactions. Structured, paid services now drive scalability, making criminal activity more accessible and harder to track. Success in these markets increasingly depends on purchased services rather than reputation or expertise, a shift that was not previously observed in Telegram-related research. This finding adds to the understanding of how Telegram continues to evolve as an illicit market.

These three observations drastically lower the barriers to entry for new actors, in combination with Telegram's search functionality which allows even low-skilled offenders without prior connections to locate criminal networks, vendors, and illicit products with minimal effort. This ease of access not only facilitates adaptability within criminal markets but also increases the likelihood that individuals using Telegram for legitimate purposes may inadvertently stumble upon or be exposed to illicit content. As a result, the normalisation of illegal activities and unintentional participation become greater risks for society. The platform's increased accessibility and automation-driven criminal infrastructure highlight the need for enforcement actions.

8.1.2 Dynamic Displacement within Telegram

The second contribution of this research draws on the concepts of crime displacement and multi-homing (cross-listing across platforms). Crime displacement is often studied in terms of criminals moving from one platform to another or switching crime types in response to enforcement actions (Moeller et al., 2017; Ouellet et al., 2022; Verburgh et al., 2018). Similarly, multihoming, where vendors cross-list products across multiple platforms to reduce risk, is a well-documented phenomenon (Ouellet et al., 2022; Vana & Pachigolla, 2021). This study builds on these concepts but provides new insights by demonstrating that there are mechanisms installed that enable dynamic displacement and multihoming within Telegram itself, rather than only across different platforms. As Telegram has very recently begun with stricter moderation, and increased collaboration with law enforcement, the exact impact on the behaviours within Telegram channels has not been researched earlier.

Initially, it could be expected that this would trigger communities to relocate to other platforms, and it could be anticipated that the overall volume of advertisements for illicit goods and services would decline due to increased fear of detection. This research shows that there is no empirical evidence of a mass exodus to other platforms. Chat messages include no discussion topics about large-scale relocation to alternative communication platforms, fear of detection, announcements of channel closure(s) or general abandonment of Telegram.

However, with the current insights from the messages, this study cannot empirically prove whether crime has truly decreased in absolute numbers or if it has simply shifted towards private group channels, encrypted one-on-one conversations, or other platforms (without this being communicated in public Telegram channels). Rather, two observations about crime adaptation can be made. First, the total number of messages, including advertisements, is significantly lower than in the reference dataset (Table 2), which is mainly due to the increased use of the auto-deletion function. Additionally, it was observed that 26 channels were closed before data collection, and seven more were shut down during the analysis phase. Two channels displayed a message stating the reason for closure; one due to a violation of Telegram's Terms of Service and another because users posted illegal pornographic content. The remaining channels did not disclose any reason and simply could no longer be found. It remains unclear whether these were voluntary shutdowns, potentially influenced by the deterrence effect, or whether they were the result of Telegram's heightened moderation efforts targeting channels within this dataset. Of the 71 identified channels that met the criteria for inclusion in this research, only 38 were still active as of early February 2025.

Although it cannot be empirically demonstrated that users abandon Telegram, mechanisms have been identified that facilitate internal crime displacement. This includes vendors and buyers quickly reconnecting in new channels due to the ease of creating and closing channels, the decentralised nature of invitation-sharing, and the widespread use of broadcasting channels that serve as navigation hubs for illicit marketplaces. Automation also enables seamless cross-listing of advertisements, allowing vendors to maintain visibility across multiple channels simultaneously. This mirrors multihoming behaviour observed in dark web markets but occurs entirely within Telegram, reinforcing its resilience as an illicit ecosystem.

These findings challenge traditional views on crime displacement by showing that rather than pushing criminals off a platform, mechanisms are installed that can lead to easier displacement within a single platform. This distinguishes this research from previous work on cross-platform displacement. As Telegram channels are shut down, actors can implement stricter gatekeeping and rely more on broadcasting channels to maintain network stability. Also, the presence of English and German chat and bot messages confirms that Telegram is not confined to national borders but rather operates as a globalised ecosystem. This shifts the landscape from open-market style trading to a more dispersed but interconnected ecosystem, making enforcement more challenging. Recognising that crime displacement and multihoming can occur within a single platform, rather than just across platforms, is critical for future research and enforcement strategies.

8.1.3 Vendor and Channel Specialisation

Last, this study provides several new insights into how specialisation, scarcity-driven demand, and payment preferences further shape illicit markets. Existing research has examined underground communities as *offender convergence settings*, where criminals interact, trade goods and services, and share knowledge (Leukfeldt et al., 2017; Paquet-Clouston & García, 2022), which holds true for Telegram. This research reveals that specialisation occurs at vendor level rather than the channel level. Contrary to expectations, most channels do not focus exclusively on specific crime types, except for those dedicated to fireworks, firearms and explosives (Figure 4). Rather, most Telegram channels feature mixed illicit offerings. Instead, 67.6% of vendors specialise in a single crime category (Figure 11), suggesting that actors either create new accounts when diversifying their offerings or refrain from expanding into new criminal domains. This indicates that, rather than functioning as traditional, structured illicit marketplaces, channels serve as broad storefronts where specialised individuals operate.

Building further on this level of specialisation, it is observed that single-category vendors prefer an average of 1.37 payment methods in their ads, whereas multi-category vendors accept an average of 1.63. This suggests that vendors operating across multiple illicit markets adopt a more flexible payment strategy to cater to a wider range of buyers and reduce transaction barriers, signalling a higher level of professionalisation. Furthermore, evidence of community adaption was observed in general payment trends (as the results from the current dataset were held against the reference dataset). While digital payment methods such as 'Tikkie' and direct bank transfers were commonly used earlier, their presence has declined significantly. This contradicts expectations that such methods would remain dominant and instead highlights an increasing reluctance among criminals to expose their real-world identities. For drugs and other physical goods, cash has become the preferred payment method, probably due to its anonymity and untraceability. However, for cybercrime and financial fraud (such as cash-out schemes), digital payments like PayPal, Paysafe, and cryptocurrencies remain prevalent, as these crimes occur entirely online, eliminating the need for in-person transactions.

Last, this study highlights how scarcity-driven demand is observed. While weapons, firearms, and fireworks are advertised less frequently, they generate a disproportionately high number of user requests (Figure 12). This suggests that when a product is harder to find, users become more proactive in seeking it out, reinforcing demand. Restricting supply by eliminating certain types of crime therefore does not mean that demand is automatically limited. Rather, it pushes buyers towards more concealed, demand-based interactions.

These findings further support the argument that Telegram should be analysed as an interconnected ecosystem rather than focusing solely on isolated channels or crime categories (Van Wegberg et al., 2020). As types of crime are exchanged interchangeably, actors witness and absorb knowledge from other actors, without direct engagement. This automated cross-category learning further strengthens Telegram's role as a decentralised, adaptable convergence space for illicit activity.

8.2 Limitations

During the analyses, several limitations emerged that affected aspects of the research. For clarity, these encountered limitations will be presented below based on the moment of encountering. Subchapters 8.2.1 and 8.2.2 respectively present the limitations found in the qualitative and quantitative approaches.

8.2.1 Limitations in the Qualitative Approach

The qualitative research has three limitations, regarding (I) the backgrounds and perspectives of the interview respondents, (II) the extent of representation of the found phenomena and concepts in literature and interviews, and (III) the lack of validation possibilities with existing literature. First, while the four interviews were conducted with experts in law enforcement, financial crime, and anti-money laundering, the perspectives of cybercriminals, financial intermediaries, and other actors are underrepresented. This creates a law enforcement-centric view, where criminal behaviour is interpreted based on detected cases and available data, rather than direct insights from offenders. As a result, actual criminal strategies may differ from those assumed in this study. Additionally, the

interviews were designed to capture a broad range of expertise rather than multiple perspectives on the same area of specialisation. Given that each respondent specialises in different aspects of criminal behaviour and investigation, their perspectives complement one another. However, this also means that findings are illustrative rather than comprehensive or universally applicable, as each interview reflects an individual viewpoint rather than a consensus across experts. This approach was intentional, as the objective of the interviews was to identify relevant concepts and contextualise findings, rather than to systematically validate the same knowledge across multiple respondents. Consequently, while the interviews provide valuable insights, they do not fully capture all perspectives within the illicit ecosystem.

Second, the frequency illusion (*Baader-Meinhof phenomenon*), which is a cognitive bias where increased attention to a phenomenon makes it appear more widespread than it is, could occur. Since the literature review and interviews focus specifically on the mechanisms driving adaptive behaviours, certain trends may seem more dominant simply because they were prioritised in research and enforcement. Additionally, law enforcement primarily detects and prosecutes known offenders, meaning observed trends may not fully capture undetected criminal migration patterns. Those who evade detection may use different tactics, leading to a skewed understanding of actual adaptations. To address this bias, the quantitative analysis was conducted extensively, ensuring conclusions are grounded in both empirical data and perceptions.

The third qualitative limitation is the lack of existing literature on criminal activity within Telegram. This study draws parallels from research on dark web communities, however, these platforms operate under different conditions. There is heavy reliance on escrow services, reputation systems, and vendor ratings, while Telegram lacks similar build-in mechanisms. Additionally, dark web participants are typically more privacy-conscious, while Telegram attracts a broader range of offenders, and dark web markets are often taken down through large-scale interventions, while Telegram-based crime is more decentralised, with authorities removing individual channels or banning accounts rather than dismantling the entire ecosystem. Therefore, existing studies do not fully cover Telegram's unique dynamics, such as the role of bots and broadcast channels, or the ease of re-starting marketplaces after shutdowns. This study filled that gap by providing empirical insights. However, without prior theoretical frameworks specific to Telegram's ecosystem, some findings, particularly those related to market structures, automation, and displacement, cannot be fully validated against existing literature.

8.2.2 Limitations in the Quantitative Approach

In the quantitative phase of this research, five limitations were encountered, regarding (I) Telegram's auto-delete and mass forwarding function, (II) differentiating correlation from causation, (III) the identification of channels and the scraping process, (IV) challenges during data classifying (using SVMs) and (V) the topic modelling process (using LDA). The first two limitations are more overarching and have more broad impacts and consequences, the last three were encountered during individual analyses and have specific impacts.

The first and most significant constraint is the impact of Telegram's auto-delete function and the mass use of automated message forwarding on the data availability and uniqueness. First, the availability of messages over time is heavily influenced by the auto-delete function that skews the dataset by disproportionately capturing messages from the last few weeks of the scraping period, leading to reduced availability of older messages and making it challenging to analyse long-term behavioural shifts. Consequently, some observed trends may reflect short-term fluctuations rather than sustained changes in criminal operations, limiting the ability to track vendor activity, listing frequency, and operational adaptations within the full period. Additionally, the machine learning models trained on recent messages may underrepresent older terminology, strategies, or trends. To counter this limitation, the study employs several mitigation strategies to improve its robustness. By incorporating a reference dataset, a comparative framework was created that allowed for assessing whether recent findings align with historical trends. Although a definitive baseline for Telegram research is still lacking, this approach ensures that insights are contextualised within broader patterns observed over time. While long-term patterns may be difficult to confirm with certainty, the study provides concrete observations, and the underlying mechanisms of how illicit actors

adapt within Telegram. Second, through the extensive use of automated forwarding of messages, the level of uniqueness in messages is drastically lower than expected (5.3%). This impacts the ability to analyse organic interactions and tailored advertisements, as most of the content is mass-distributed, pre-written, and impersonal. This overrepresentation of duplicate messages affects the reliability of descriptive statistics for message types, advertisement categories, and payment preferences. The implications of this limitation have been further mitigated by employing not only analysed based on the offer and request advertisements but also by using chat and bot messages. And, by comparing findings with the reference dataset, it was possible to assess whether the observed decrease in message uniqueness constituted a recent trend or a structural characteristic of illicit Telegram activity. This issue is not unique to this study, as similar challenges exist in current Telegram research. Therefore, a reflection (Chapter 8.3) on both this study and existing (broader) Telegram research is added.

A second overarching limitation of this study is the challenge of distinguishing correlation from causation when analysing the interaction between users, the found systemic mechanisms and the impact on individuals and Telegram as a marketplace. This issue arises because the research is based on scraped messages rather than direct transactional data or firsthand input from actors within the ecosystem. As a result, it is difficult to determine whether advertisements lead to actual sales and whether shifts in community behaviours are direct responses to external pressures, such as enforcement actions and platform moderation, rather than internal factors like market evolution or changing user preferences. For example, while the observed extensive closure of Telegram channels closely followed Telegram's announcement of increased law enforcement cooperation, alternative explanations such as internal disputes, migration to other platforms (without disclosing this), or a shift to private encrypted chats cannot be ruled out entirely. Similarly, changes in *modi operandi*, such as the decline in cryptocurrency payments and the increased use of auto-delete and message-forwarding functions, could be reactions to enforcement pressures but may also stem from evolving criminal business models, user preferences, or innovation. To mitigate this limitation, this research mainly places focus on examining the mechanisms that enable behavioural change within communities rather than directly measuring behavioural adaptation at an individual level. Where possible, trends were supported by empirically demonstrable shifts in *modi operandi* observed across the ecosystem. Additionally, multiple validation strategies were applied, including using literature and expert interviews to place the found concepts into context, and comparing trends with the reference dataset. While proving direct causation remains challenging, the study provides strong empirical evidence that Telegram-based criminal networks are evolving in response to enforcement measures in a structured and adaptive manner.

Third, various design choices during the channel identification and scraping process had an impact on later found insights. The selected timeframe and the channels that have been scraped only capture a snapshot of the Dutch evolving criminal ecosystem within Telegram. The snowball method for identifying groups may thereby have introduced selection bias. As channels were partly discovered through links shared within already-identified channels, certain types of groups may have been overrepresented, while others remained undiscovered. While it was affirmed that most channels offer a variety of products and/or services, this could have influenced the observed *modi operandi*, potentially underrepresenting less visible or more hidden criminal communities or crime types within Telegram. Additionally, this research did not incorporate messages originating from private channels or one-on-one conversations, where deals are likely finalised. Building on the mentioned quantitative limitation, this means that while the analysis provides insights into what is offered, it does not confirm whether transactions occur. The same applies to the payment preferences, as they reflect stated preferences rather than actual transaction records, making it difficult to determine which methods are truly used. Furthermore, the decision was made not to include media in the analyses, due to four reasons. First, this would exponentially increase the storage needs, it would require considerable manual effort to analyse such content, it offers minimal additional insights necessary for addressing the current research questions and presents a substantial risk of acquiring explicit data, such as revenge and/or child pornography. However, without incorporating additional channels, one-on-one conversations and without media, this study successfully captured ecosystemic trends.

Fourth, in the message classification process, certain categories and message types emerged that were more challenging to fit, resulting in lower accuracy rates. Since the study builds on the classified messages, a small margin of error will always persist in subsequent analyses, potentially affecting the precision of certain findings. This does not pose significant issues for most categories. However, some implications of misclassification have been observed. This paragraph will highlight both limitations in the model with advertisement categories and message types. First, the model struggled with specific crime categories: Weapons, Firearms and Explosives, Stolen Goods, and 'Other', as displayed in Appendix D. This is due to their low representation in the labelled dataset and high variability within these messages, which could lead to underrepresentation where categories may appear less prevalent than they are. Pharmaceuticals were frequently misclassified under soft and hard drugs, as they were often advertised together in the same message, making category distinction more difficult. The implications of these misclassifications are minimal. The overall precision and recall of this first model are comparable to, or even exceed, those of similar studies employing the same methodologies and equivalent datasets. The absolute number of misclassified cases is small, however, it is essential to have caution when using these classifications in subsequent analyses. Regarding the classification model that determined message types, chat messages had a higher misclassification rate, with 11% of chat messages being incorrectly labelled as offer advertisements and 11% being classified as request advertisements. This misclassification led to a reduced accuracy of the topic modelling analysis. Although it was also observed that offer advertisements were classified as request advertisements, or vice versa, this misclassification is less severe. The advertisements are still utilised within the appropriate analyses. However, misclassification into an entirely different category results in these messages not being included in the correct analysis. The model used for chat messages was developed using a dataset that therefore excluded the messages categorised as advertisements, despite their actual nature as chat messages, reducing its ability to extract all conversational topics. This suggests that there could be more topics present in the data than initially identified in Chapter 6.3. However, by building on the reference dataset, a better perspective was generated. Expanding the labelled dataset for underrepresented categories with a larger variety of messages, could improve classification accuracy in the future.

Last, during the topic modelling process, various other limitations were encountered. First, the coherence scores for the model with chat messages were lower than expected, making it more challenging to fit topics to clearly defined latent subjects. This issue is partly due to the short, informal, and high variability of Telegram messages. Many messages lack sufficient context or structure, making it difficult for the model to extract meaningful topics. The dataset contained 5,488 unique tokens after preprocessing, significantly fewer than in similar studies. This limited vocabulary reduces the diversity and richness of the extracted topics, reducing the model's ability to identify nuanced themes. A larger dataset with more chat messages would likely improve topic coherence and provide clearer insights into criminal discussions. Second, the results from the LDA did not indicate that crime is displaced beyond Telegram. Activity that may have moved to non-public or more secure communication channels it therefore not captured. While several Telegram groups were observed shutting down, this does not necessarily indicate migration to other platforms. Instead, criminals may have adopted tighter security measures, may have shifted to other digital platforms (without disclosing this) or may have held operational pauses.

8.3 Reflection & Future Research

This study has provided insights into overarching trends within Telegram's illicit market, rather than providing a wide snapshot of criminal activity between 2021 and 2024. The findings emphasise the heavily commoditised nature of the platform, where automation and mass forwarding of messages shape the communities' structure. One of the key contributions of this research is highlighting the shift from Telegram as a chat-based environment toward a market driven by duplicates and automated interactions. Previous studies have focused on Telegram communities, but few have accounted for the extent to which message automation influences research design and its findings.

The way data is collected and processed plays a crucial role in shaping research outcomes. Factors such as the selection of channels, time dedicated to identifying new channels, the chosen timeframe, and especially the frequency of scraping directly impact the observed channel and message descriptives. For example, weekly

scraping could offer a better understanding of the evolving market dynamics. Additionally, deduplication methods influence whether findings reflect actual supply and demand or are skewed by bot-driven advertisement cycles. Rather than viewing the high level of duplicate messages solely as a limitation, it is argued that it should be understood as evidence of a structural change in how illicit actors operate on Telegram. However, the extensive use of repeated messages makes it more challenging to analyse *modi operandi* longitudinally. The visibility of crime categories has shifted from organic supply to the extent of how much vendors invest in message automation and promotion. In contrast, request advertisements and chat-based interactions appear to occur more organically, offering valuable insights into genuine user behaviour.

This study provides a foundation for understanding Telegram's evolving illicit market, but several key areas remain unexplored. Future research should adopt a market-oriented approach, recognising Telegram as an automated advertising hub rather than a socially driven marketplace. Refining scraping methods, tracking internal displacement, and analysing automation mechanisms will result in new insights into platform dynamics.

First, a crucial next step is tracking internal crime displacement within Telegram. Continuous or periodic scraping can be used to monitor channel closures and channel launches. Mutually shared invitation links thereby allow researchers to generate network graphs, and see which (broadcasting) channels function as central hubs. Further analysis is also needed on bot-driven automation. This study identifies automation as a core feature, but bot frequency, pricing, functionality, and general reliance on automation remain unclear. Future research could map message timestamps, ad duplication rates, and bot behaviours to distinguish between human-driven and fully automated content distribution. To capture long-term trends versus short-term fluctuations, weekly scheduled scraping could mitigate the effects of the auto-delete function. In the current dataset, the messages are scraped without capturing the origin of forwarded messages. Future research should trace forwarded messages to identify central broadcasting hubs and uncover cross-channel vendor networks. Understanding how vendors distribute ads across multiple groups would help pinpoint key facilitators within Telegram's cybercriminal ecosystem. Also, further analysis can be conducted on the interim findings (results derived from intermediate analyses), as this research uses those results to discover trends, but does not dive deeper into these specifically. Analysis of vendor specialisation and payment strategies could provide additional insights into criminal professionalism. This study suggests that vendors accepting multiple payment methods show higher adaptability, but linking advertisement patterns, payment trends, and vendor profiles could further distinguish between professionalised cybercriminals and casual sellers. Last, establishing benchmark datasets for long-term comparisons would allow researchers to track Telegram's market evolution, distinguishing temporary enforcement effects from structural changes. Addressing these gaps will refine our understanding of Telegram's resilience and the mechanisms sustaining its illicit markets.

8.4 Recommendations

This chapter presents recommendations for law enforcement agencies and policy makers. Law enforcement agencies can benefit from differentiating targeting strategies, which are elaborated upon first. First, traditional enforcement strategies need to be adapted for Telegram as a market. Closing individual Telegram channels has proven ineffective due to the ease with which vendors can reopen new ones, attract members, and resume operations. Instead of focusing on reactive takedowns, enforcement should target the underlying market mechanisms that sustain illicit trade. Reduced reliance on self-regulation strategies such as scam registries, blacklists, and invitation-based access limits the ability to maintain trust and security. By prioritising dismantling these trust mechanisms, uncertainty and operational instability are introduced.

Second, law enforcement should place greater focus on disrupting automation and commoditised services that facilitate illicit activities. Vendors no longer rely on organic interactions but instead use automation mechanisms to maximise their reach. Identifying key bot developers from which their services are used for illicit purposes would reduce the exposure of illicit content. Besides, building on broadcasting channels and forwarded messages,

enforcement should focus on monitoring and dismantling central broadcasting channels, as these serve as central hubs that direct users to illicit groups.

Third, increased enforcement does not necessarily drive criminals off Telegram; instead, it can force them to migrate to more private settings. Many now shift to private invite-only groups or encrypted one-on-one chats rather than leaving the platform altogether. Enforcement strategies should account for this pattern and place attention on infiltrating these channels. Furthermore, when certain crime types become harder to find due to takedowns, user demand increases as buyers proactively search for new supply. This indicates that restricting supply does not eliminate demand but instead shifts to demand-based interactions, and potentially to less visible spaces.

Fourth, law enforcement strategies could benefit from tailoring strategies based on user types. Oblivious users remain largely unaware of enforcement actions and continue engaging in illicit activities as long as they have access to active vendors and payment systems. Awareness campaigns and deterrence-based strategies may be effective in discouraging their participation. On the other hand, cautious and professional users anticipate law enforcement measures and proactively adjust their security practices, either by increasing operational secrecy or relocating to more private Telegram spaces. Targeting this group requires dismantling trust-building mechanisms such as scam registries, verification services, and invitation-based vetting.

Last, while Telegram has taken steps to increase moderation and remove non-compliant channels, further collaboration with law enforcement could improve proactive crime detection. Monitoring emerging channels, tracking high-risk accounts, and sharing intelligence on reported messages. Also, Telegram's API currently provides an underutilised opportunity to track illicit activities in real-time. Monitoring high-risk keywords, new channel creations, administrator accounts, and repeated advertisement patterns can provide valuable insights for disrupting criminal networks before they fully establish themselves. By shifting towards predictive and proactive monitoring rather than reactive enforcement, enforcement agencies can gain an upper hand in cybercrime prevention.

Policy makers could also benefit from various recommendations. Current legal frameworks do not always clearly define when passive membership in a criminal group constitutes illegal activity, leaving grey areas in enforcement. A key policy recommendation is to make legal definitions regarding the criminal liability of users who join illicit Telegram channels but do not actively engage in illegal transactions clearer. Merely being in a group without making purchases, sales, or promotions is usually not directly punishable. Regulatory bodies and law enforcement should focus on raising awareness among users who unknowingly interact with these networks, emphasising the risks and potential legal consequences of engagement. The same grey areas can be observed in dual-use tools, where services designed for legitimate purposes (such as automated moderation, message distribution and anti-spam filters) are repurposed to facilitate illicit activities. Such providers should be forced to implement more proactive monitoring mechanisms and ethical safeguards to detect and prevent the misuse of their services within criminal ecosystems. Also, the regulatory framework governing such services must be strengthened. The shutdown of a single service, as observed in the case of Tornado Cash (as noted in the interviews), quickly led to the emergence of similar services.

9 Conclusion

In this research, the research gap identified in Chapter 2.2 was addressed by exploring the primary research question: *What ecosystemic mechanisms stimulate the resilience of Telegram as an illicit market?* This was achieved through a combination of qualitative and quantitative methodologies. The qualitative component, which included expert interviews and a comprehensive literature review, laid the groundwork and provided a theoretic lens for the subsequent quantitative phase. This phase involved the use of 1.4M independent sources from 2021 and 2024, revealing patterns of adaptive behaviour, trends in payment methods, self-incurred safety measures and displacement dynamics within the Dutch cybercriminal landscape.

This study revealed that Telegram's criminal ecosystem operates through a service-based economy, where automation and outsourcing drive efficiency, scalability, and resilience against enforcement. Users and administrators exploit Telegram's technological features to automate and scale illicit activities, transforming the platform into a structured and self-sustaining marketplace. Bots play a crucial role in this process, performing tasks such as auto-deletion, message forwarding, scam detection, access control through gatekeeping systems, and channel moderation. Auto-deletion mechanisms significantly impact data retention, erasing messages after set timeframes, and attempting to minimise illicit exposure to law enforcement. This is evident in the dataset, where the vast majority of messages originate from the last two weeks before scraping. The commoditisation of marketing services allows vendors to outsource advertisement distribution, ensuring their listings are distributed in bulk rather than being tailored to audiences, ensuring cross-listing across multiple channels with minimal effort. These mechanisms result in a significant decline in message uniqueness, with only 5.3% of messages being unique (compared to 21.8% in the reference dataset (2017-2021)), mainly impacted by the high level of standardisation in offer advertisements and bot messages. Meanwhile, administrators further use self-regulating enforcement tools, such as scam registries and blacklists, to maintain order and trust within illicit communities. These automation-driven mechanisms shift Telegram away from traditional one-on-one criminal interactions and socially driven communication platform toward a heavily commoditised illicit advertising ecosystem.

Despite dozens of observed channel closures, chat messages empirically confirmed that there are no large-scale discussions about migrating to alternative platforms, contradicting potential expectations of a mass exodus. Combined with the significantly lower total number of messages than in the reference dataset, a strong deterrence effect can still be derived. However, it is empirically indeterminable whether and to what extent criminal activity overall on Telegram has decreased in response to the increased moderation efforts and collaboration with law enforcement. Nevertheless, mechanisms are observed that can provide resilience to the market. This is primarily sustained through dynamic displacement within Telegram and the strategic use of broadcasting channels and gatekeeping systems. Rather than migrating to alternative platforms, mechanisms are provided that enable rapid relocating within Telegram itself. Invitation-based access systems allow communities to maintain exclusivity, attempting to filter out potential threats while simultaneously expanding their reach through link-sharing requirements. Besides, broadcasting channels function as central hubs, ensuring that even when well-known channels are shut down, vendors and buyers can reconnect quickly.

Specialisation within Telegram's illicit ecosystem occurs primarily at the vendor level rather than the channel level. Most channels do not specialise in a single crime type, except for a few categories, such as weapons and fireworks. Instead, Telegram channels act as general storefronts, where vendors with diverse offerings coexist. This lack of strict channel specialisation makes enforcement more challenging, as illicit goods and services are dispersed across multiple spaces rather than being confined to distinct, easily targetable groups. At the vendor level, 67.6% of sellers specialise in a single crime category. Multi-category vendors (32.4%) demonstrate professionalism to an extent by accepting a greater variety of payment methods (1.63 on average vs. 1.37 for single-category vendors), ensuring flexibility in transactions. This suggests that more experienced actors strategically diversify their offerings and payment options to maximise reach. For buyers, this structure influences how they engage with the illicit market. Since most channels are not specialised, users must navigate multiple groups or rely on broadcasting channels to

find specific goods. When enforcement actions target certain products, illicit trade does not disappear; instead, buyers shift to demand-driven interactions, increasing the prevalence of request advertisements. This is particularly evident in scarcity-driven markets, such as (fire)weapons and fireworks, where fewer advertisements correlate with a higher number of user requests. When supply becomes constrained, whether due to enforcement efforts or shifts in vendor activity, buyers become more proactive in seeking out alternatives. Ultimately, the combination of non-specialised channels, vendor expertise, and demand-driven market shifts ensures that Telegram's illicit economy remains resilient, decentralised, and difficult to dismantle. Furthermore, it is observed that drug-related transactions have shifted from cryptocurrency to cash, which is likely due to physical exchanges and pre-existing in-person contact. Cybercrime and financial fraud increasingly favour digital payment methods, such as PayPal and Paysafecard, due to their perceived anonymity. However, the use of legitimate but identifiable payment services like 'Tikkie' and bank transfers has declined, reflecting growing caution among vendors.

To sum up and address the main research question, mechanisms are observed that have transformed Telegram from a communication platform to a commoditised, automated and adaptive platform. With reduced organic interaction. Automation minimises the need for social ties and replaces traditional trust mechanisms. Bots facilitate large-scale message distribution, moderation, and self-regulation, ensuring market efficiency while attempting to reduce exposure to law enforcement allowing illicit trade to operate efficiently without the need for deep social ties or trust-based networks. Internal displacement mechanisms, including invitation-based gatekeeping and broadcasting channels, allow actors to relocate and re-establish operations within Telegram rather than abandon the platform entirely and maintain the continuity of communities. Specialisation among vendors, and limited channel specialisation, strengthen market adaptability, ensuring continued access to illicit products despite enforcement efforts. Together, these mechanisms create a highly dynamic ecosystem where illicit trade persists, not through static structures, but through continuous adaptation and resilience in response to external pressures. To break this trend, law enforcement is recommended to target automation and bot networks, disrupting trust-building mechanisms, and monitor broadcasting hubs, shifting focus from reactive takedowns to proactive intelligence. Policy suggestions emphasise clarifying criminal liability for passive group membership, regulating dual-use automation services, and strengthening platform collaboration.

References

- Aggarwal, C. C., & Zhai, C. (2012). A Survey of Text Classification Algorithms. In C. C. Aggarwal & C. Zhai (Eds.), *Mining Text Data* (pp. 163–222). Springer US. https://doi.org/10.1007/978-1-4614-3223-4_6
- Akyazi, U., van Eeten, M. J. G., & Hernandez Ganan, C. (2021). *Measuring Cybercrime as a Service (CaaS) Offerings in a Cybercrime Forum: Workshop on the Economics of Information Security*.
- Aldridge, J., & Askew, R. (2017). Delivery dilemmas: How drug cryptomarket users identify and seek to reduce their risk of detection by law enforcement. *International Journal of Drug Policy*, 41, 101–109. <https://doi.org/10.1016/j.drugpo.2016.10.010>
- Aldridge, J., & Decary-Hetu, D. (2015). Cryptomarkets and the future of illicit drug markets. In *The Internet and Drug markets* (pp. 23–32). Publications Office of the European Union. <https://doi.org/10.2810/324608>
- Alloghani, M., Al-Jumeily, D., Mustafina, J., Hussain, A., & Aljaaf, A. J. (2020). A Systematic Review on Supervised and Unsupervised Machine Learning Algorithms for Data Science. In M. W. Berry, A. Mohamed, & B. W. Yap (Eds.), *Supervised and Unsupervised Learning for Data Science* (pp. 3–21). Springer International Publishing. https://doi.org/10.1007/978-3-030-22475-2_1
- Altinok, D. (2021). *Mastering spaCy: An end-to-end practical guide to implementing NLP applications using the Python ecosystem*. Packt Publishing Ltd.
- AMLC. (2024, September 12). *Witwassen en cryptovaluta*. AMLC. <https://www.amlc.nl/witwassen-en-cryptovaluta/>
- Amoo, O. O., Atadoga, A., Abrahams, T. O., Farayola, O. A., Osasona, F., & Ayinla, B. S. (2024). The legal landscape of cybercrime: A review of contemporary issues in the criminal justice system. *World Journal of Advanced Research and Reviews*, 21(2), 205–217. <https://doi.org/10.30574/wjarr.2024.21.2.0438>
- Armona, L. (2018). *Measuring the Demand Effects of Formal and Informal Communication: Evidence from Online Markets for Illicit Drugs* (arXiv:1802.08778). arXiv. <https://doi.org/10.48550/arXiv.1802.08778>
- Baraz, A., & Montasari, R. (2023). Law Enforcement and the Policing of Cyberspace. In *Digital Transformation in Policing: The Promise, Perils and Solutions* (pp. 59–83). Springer; Scopus. https://doi.org/10.1007/978-3-031-09691-4_4
- Barratt, M. J., & Aldridge, J. (2016). Everything you always wanted to know about drug cryptomarkets* (*but were afraid to ask). *International Journal of Drug Policy*, 35, 1–6. <https://doi.org/10.1016/j.drugpo.2016.07.005>
- Basheer, R. (2022). Cryptomarkets' Phenomenon: A Conceptualization Approach. *Human Behavior and Emerging Technologies*, 2022(1), 6314913. <https://doi.org/10.1155/2022/6314913>
- Beerthuizen, M., Sipma, T., & Laan, A. M. (2020). *Aard en omvang van dader- en slachtofferschap van cyber- en gedigitaliseerde criminaliteit in Nederland*.
- Bijlenga, N., & Kleemans, E. R. (2018). Criminals seeking ICT-expertise: An exploratory study of Dutch cases. *European Journal on Criminal Policy and Research*, 24(3), 253–268. <https://doi.org/10.1007/s10610-017-9356-z>
- Blei, D. M., Ng, A. Y., & Jordan, M. I. (2003). Latent dirichlet allocation. *J. Mach. Learn. Res.*, 3(null), 993–1022.
- Boekhout, H. D., Blokland, A. A. J., & Takes, F. W. (2024). Early warning signals for predicting cryptomarket vendor success using dark net forum networks. *Scientific Reports*, 14(1), 16336. <https://doi.org/10.1038/s41598-024-67115-5>
- Boersma, K. (2023). *So long and thanks for all the (big) fish: Exploring cybercrime in Dutch Telegram groups* [Info:eu-repo/semantics/masterThesis, University of Twente]. <https://essay.utwente.nl/96173/>
- Bosman, T. (2025, January 7). Jongen (16) sprak bij Ikea af voor grote Cobra-deal, maar bleek zaken te doen met een undercoveragent. *AD.nl*. <https://www.ad.nl/binnenland/jongen-16-sprak-bij-ikea-af-voor-grote-cobra-deal-maar-bleek-zaken-te-doen-met-een-undercoveragent-ad7e168a/>

- Cabrero-Holgueras, J., & Pastrana, S. (2021). A Methodology For Large-Scale Identification of Related Accounts in Underground Forums. *Computers & Security*, 111, 102489. <https://doi.org/10.1016/j.cose.2021.102489>
- Chang, J., Gerrish, S., Wang, C., Boyd-graber, J., & Blei, D. (2009). Reading Tea Leaves: How Humans Interpret Topic Models. *Advances in Neural Information Processing Systems*, 22. https://proceedings.neurips.cc/paper_files/paper/2009/hash/f92586a25bb3145facd64ab20fd554ff-Abstract.html
- Chayka, K. (2024, September 4). The Arrest of Telegram's Founder Illuminates Global Anxieties About Social Platforms. *The New Yorker*. <https://www.newyorker.com/culture/infinite-scroll/the-arrest-of-telegrams-founder-illuminates-global-anxieties-about-social-platforms>
- Chen, C., Peersman, C., Edwards, M., Ursani, Z., & Rashid, A. (2021). AMoC: A Multifaceted Machine Learning-based Toolkit for Analysing Cybercriminal Communities on the Darknet. In Chen Y., Ludwig H., Tu Y., Fayyad U., Zhu X., Hu X.T., Byna S., Liu X., Zhang J., Pan S., Papalexakis V., Wang J., Cuzzocrea A., & Ordonez C. (Eds.), *Proc. - IEEE Int. Conf. Big Data, Big Data* (pp. 2516–2524). Institute of Electrical and Electronics Engineers Inc.; Scopus. <https://doi.org/10.1109/BigData52589.2021.9671906>
- Chua, Y. T., & Wilson, L. (2023). Beyond Black and White: The Intersection of Ideologies in Online Extremist Communities. *European Journal on Criminal Policy and Research*, 29(3), 337–354. Scopus. <https://doi.org/10.1007/s10610-023-09555-9>
- Collier, B., Thomas, D. R., Clayton, R., Hutchings, A., & Chua, Y. T. (2022). Influence, infrastructure, and recentering cybercrime policing: Evaluating emerging approaches to online law enforcement through a market for cybercrime services. *Policing and Society*, 32(1), 103–124. <https://doi.org/10.1080/10439463.2021.1883608>
- Combot Anti-Spam System. (n.d.). *Combot Anti-Spam System (CAS)*. Retrieved January 29, 2025, from <https://cas.chat/>
- Creswell, J. W. (2009). *Research design: Qualitative, quantitative, and mixed methods approaches*, 3rd ed (pp. xxix, 260). Sage Publications, Inc.
- Cugler, E. (2024). *Web Scraping Telegram Posts and Content* [Computer software]. https://github.com/ergoncugler/web-scraping-telegram/blob/main/combine_scraped_parquet_files.py
- De Rechtspraak. (2024, May 14). *Ontwikkelaar van Tornado Cash gaat cel in voor witwassen van miljarden dollars aan cryptovaluta*. <https://www.rechtspraak.nl/Organisatie-en-contact/Organisatie/Rechtbanken/Rechtbank-Oost-Brabant/Nieuws/Paginas/Ontwikkelaar-van-Tornado-Cash-gaat-cel-in-voor-witwassen-van-miljarden-dollars-aan-cryptovaluta.aspx>
- Décary-Héty, D., & Giommoni, L. (2017). Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous. *Crime Law and Social Change*, 67. <https://doi.org/10.1007/s10611-016-9644-4>
- Deliu, I., Leichter, C., & Franke, K. (2018). Collecting Cyber Threat Intelligence from Hacker Forums via a Two-Stage, Hybrid Process using Support Vector Machines and Latent Dirichlet Allocation. *2018 IEEE International Conference on Big Data (Big Data)*, 5008–5013. <https://doi.org/10.1109/BigData.2018.8622469>
- Demant, J., Munksgaard, R., Décary-Héty, D., & Aldridge, J. (2018). Going Local on a Global Platform: A Critical Analysis of the Transformative Potential of Cryptomarkets for Organized Illicit Drug Crime. *International Criminal Justice Review*, 28(3), 255–274. <https://doi.org/10.1177/1057567718769719>
- Devlin, C., Chadwick, S., Moret, S., Baechler, S., Rossy, Q., & Morelato, M. (2024). Illuminating the dark web market of fraudulent identity documents and personal information: An international and Australian perspective. *Forensic Science International*, 363. Scopus. <https://doi.org/10.1016/j.forsciint.2024.112203>

- Du, K. (2022, March). (PDF) Evaluating Hyperparameter Alpha of LDA Topic Modeling. *ResearchGate*.
<https://doi.org/10.5281/zenodo.6327965>
- Du, P.-Y., Zhang, N., Ebrahimi, M., Samtani, S., Lazarine, B., Arnold, N., Dunn, R., Suntwal, S., Angeles, G., Schweitzer, R., & Chen, H. (2018). Identifying, Collecting, and Presenting Hacker Community Data: Forums, IRC, Carding Shops, and DNMs. *2018 IEEE International Conference on Intelligence and Security Informatics (ISI)*, 70–75. <https://doi.org/10.1109/ISI.2018.8587327>
- Durrett, G., Kummerfeld, J. K., Berg-Kirkpatrick, T., Portnoff, R. S., Afroz, S., McCoy, D., Levchenko, K., & Paxson, V. (2017). Identifying Products in Online Cybercrime Marketplaces: A Dataset for Fine-grained Domain Adaptation. *Proceedings of the 2017 Conference on Empirical Methods in Natural Language Processing*, 2598–2607. <https://doi.org/10.18653/v1/D17-1275>
- Eaton, K., Stritzke, W., & Ohan, J. (2019). Using Scribes in Qualitative Research as an Alternative to Transcription. *Qualitative Report*, 24, 586–605. <https://doi.org/10.46743/2160-3715/2019.3473>
- Ebeid, I. A., & Arango, J. M. (2016). *Mallet vs GenSim: Topic Modeling Evaluation Report*.
<https://doi.org/10.13140/RG.2.2.19179.39205/1>
- European Commission. (n.d.). *Internal Policies: Cybercrime*. European Commission. Retrieved September 13, 2024, from https://home-affairs.ec.europa.eu/policies/internal-security/cybercrime_en
- Europol. (2023, June 20). *Money Muling*. Europol. <https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/money-muling>
- Frank, R., & Mikhaylov, A. (2020). Beyond the ‘Silk Road’: Assessing Illicit Drug Marketplaces on the Public Web. In M. A. Tayebi, U. Glässer, & D. B. Skillicorn (Eds.), *Open Source Intelligence and Cyber Crime: Social Media Analytics* (pp. 89–111). Springer International Publishing. https://doi.org/10.1007/978-3-030-41251-7_4
- Garkava, T., Moneva, A., & Leukfeldt, E. R. (2024). Stolen data markets on Telegram: A crime script analysis and situational crime prevention measures. *Trends in Organized Crime*. <https://doi.org/10.1007/s12117-024-09532-6>
- Gurdiel, L. P., Mediano, J. M., & Quintero, J. A. C. (2021). *A comparison study between coherence and perplexity for determining the number of topics in practitioners interviews analysis*. IV CONGRESO IBEROAMERICANO AJICEDE.
- Hou, Y., Wang, H., & Wang, H. (2022). Identification of Chinese dark jargons in Telegram underground markets using context-oriented and linguistic features. *Information Processing and Management*, 59(5). Scopus. <https://doi.org/10.1016/j.ipm.2022.103033>
- Huang, D. Y., Aliapoulos, M. M., Li, V. G., Invernizzi, L., Bursztein, E., McRoberts, K., Levin, J., Levchenko, K., Snoeren, A. C., & McCoy, D. (2018). Tracking Ransomware End-to-end. *2018 IEEE Symposium on Security and Privacy (SP)*, 618–631. <https://doi.org/10.1109/SP.2018.00047>
- Huang, K., Siegel, M., & Madnick, S. (2018). Systematically Understanding the Cyber Attack Business: A Survey. *ACM Comput. Surv.*, 51(4), 70:1-70:36. <https://doi.org/10.1145/3199674>
- Hughes, J., Aycock, S., Caines, A., Buttery, P., & Hutchings, A. (2020). Detecting Trending Terms in Cybersecurity Forum Discussions. In W. Xu, A. Ritter, T. Baldwin, & A. Rahimi (Eds.), *Proceedings of the Sixth Workshop on Noisy User-generated Text (W-NUT 2020)* (pp. 107–115). Association for Computational Linguistics. <https://doi.org/10.18653/v1/2020.wnut-1.15>
- Hughes, J., Collier, B., & Hutchings, A. (2019). From playing games to committing crimes: A multi-technique approach to predicting key actors on an online gaming forum. *2019 APWG Symposium on Electronic Crime Research (eCrime)*, 1–12. <https://doi.org/10.1109/eCrime47957.2019.9037586>

- Hughes, J., Pastrana, S., Hutchings, A., Afroz, S., Samtani, S., Li, W., & Santana Marin, E. (2024). The Art of Cybercrime Community Research. *ACM Comput. Surv.*, 56(6), 155:1-155:26. <https://doi.org/10.1145/3639362>
- Hutchings, A. (2014). Crime from the keyboard: Organised cybercrime, co-offending, initiation and knowledge transmission. *Crime, Law and Social Change*, 62(1), 1–20. <https://doi.org/10.1007/s10611-014-9520-z>
- Interpol. (2022, January 13). Combating virtual assets-based money laundering and crypto-enabled crime: Recommendations of the Tripartite Working Group on Criminal Finances and Cryptocurrencies. *Basel Institute on Governance*. 5th Global Conference on Criminal Finances and Cryptocurrencies. <https://baselgovernance.org/publications/combating-virtual-assets-based-money-laundering-and-crypto-enabled-crime>
- Jardine, E. (2021). Policing the Cybercrime Script of Darknet Drug Markets: Methods of Effective Law Enforcement Intervention. *American Journal of Criminal Justice*, 46(6), 980–1005. Scopus. <https://doi.org/10.1007/s12103-021-09656-3>
- Jardine, E., Cruz, S., & Kissel, H. (2023). Media coverage of darknet market closures: Assessing the impact of coverage on US search and Tor use activity. *Crime, Law and Social Change*, 79(3), 263–289. <https://doi.org/10.1007/s10611-022-10046-x>
- Kober, J., Bagnell, J. A., & Peters, J. (2013). Reinforcement learning in robotics: A survey. *The International Journal of Robotics Research*, 32(11), 1238–1274. <https://doi.org/10.1177/0278364913495721>
- Korenien, T., Laurikkala, J., Järvelin, K., & Juhola, M. (2004). Stemming and lemmatization in the clustering of finnish text documents. *Proceedings of the Thirteenth ACM International Conference on Information and Knowledge Management*, 625–633. <https://doi.org/10.1145/1031171.1031285>
- Krikhaar, K. (2024, October 11). *Telegram deelt voor het eerst data met Nederlandse Openbaar Ministerie*. Tweakers. <https://tweakers.net/nieuws/228558/telegram-deelt-voor-het-eerst-data-met-nederlandse-openbaar-ministerie.html>
- Kruisbergen, E. W., Leukfeldt, E. R., Kleemans, E. R., & Roks, R. A. (2019). Money talks money laundering choices of organized crime offenders in a digital age. *Journal of Crime and Justice*, 42(5), 569–581. <https://doi.org/10.1080/0735648X.2019.1692420>
- Kühn, P., Wittorf, K., & Reuter, C. (2024). Navigating the Shadows: Manual and Semi-Automated Evaluation of the Dark Web for Cyber Threat Intelligence. *IEEE Access*, 12, 118903–118922. IEEE Access. <https://doi.org/10.1109/ACCESS.2024.3448247>
- Kuzuno, H., & Tziakouris, G. (2018). Ad-hoc analytical framework of bitcoin investigations for law enforcement. *IEICE Transactions on Information and Systems*, E101D(11), 2644–2657. Scopus. <https://doi.org/10.1587/transinf.2017ICP0007>
- Ladegaard, I. (2018). We Know Where You Are, What You Are Doing and We Will Catch You. *The British Journal of Criminology*, 58(2), 414–433. <https://doi.org/10.1093/bjc/azx021>
- Ladegaard, I. (2019). Crime displacement in digital drug markets. *International Journal of Drug Policy*, 63, 113–121. <https://doi.org/10.1016/j.drugpo.2018.09.013>
- Ladegaard, I. (2020). Open Secrecy: How Police Crackdowns and Creative Problem-Solving Brought Illegal Markets out of the Shadows. *Social Forces*, 99(2), 532–559. <https://doi.org/10.1093/sf/soz140>
- Lee, W., & Seo, K. (2022). Downsampling for Binary Classification with a Highly Imbalanced Dataset Using Active Learning. *Big Data Research*, 28, 100314. <https://doi.org/10.1016/j.bdr.2022.100314>
- Leukfeldt, R., Kleemans, E., & Stol, W. (2017). The Use of Online Crime Markets by Cybercriminal Networks: A View From Within. *American Behavioral Scientist*, 61(11), 1387–1402. <https://doi.org/10.1177/0002764217734267>

- Leuprecht, C., Jenkins, C., & Hamilton, R. (2022). Virtual money laundering: Policy implications of the proliferation in the illicit use of cryptocurrency. *Journal of Financial Crime*, 30(4), 1036–1054. <https://doi.org/10.1108/JFC-07-2022-0161>
- Lonami. (2021, October 21). *Answer to “Telethon—Many messages have views=None”* [Online post]. Stack Overflow. <https://stackoverflow.com/a/69662360>
- Macdonald, M., & Frank, R. (2017). The network structure of malware development, deployment and distribution. *Global Crime*, 18(1), 49–69. <https://doi.org/10.1080/17440572.2016.1227707>
- Macdonald, M., Frank, R., Mei, J., & Monk, B. (2015). Identifying Digital Threats in a Hacker Web Forum. *Proceedings of the 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2015*, 926–933. <https://doi.org/10.1145/2808797.2808878>
- Mador, Z. (2021). Keep the dark web close and your cyber security tighter. *Computer Fraud and Security*, 2021(1), 6–8. Scopus. [https://doi.org/10.1016/S1361-3723\(21\)00006-3](https://doi.org/10.1016/S1361-3723(21)00006-3)
- Manky, D. (2013). Cybercrime as a service: A very modern business. *Computer Fraud & Security*, 2013(6), 9–13. [https://doi.org/10.1016/S1361-3723\(13\)70053-8](https://doi.org/10.1016/S1361-3723(13)70053-8)
- Meng, X. (2013). Scalable Simple Random Sampling and Stratified Sampling. *Proceedings of the 30th International Conference on Machine Learning*, 531–539. <https://proceedings.mlr.press/v28/meng13a.html>
- Moeller, K., Munksgaard, R., & Demant, J. (2017). *Flow My FE the Vendor Said: Exploring Violent and Fraudulent Resource Exchanges on Cryptomarkets for Illicit Drugs*. 61(11), 1427–1450. <https://doi.org/10.1177/0002764217734269>
- Motoyama, M., McCoy, D., Levchenko, K., Savage, S., & Voelker, G. M. (2011). An analysis of underground forums. *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference*, 71–80. <https://doi.org/10.1145/2068816.2068824>
- NOS. (2024, January 25). *Miljoenen drugsadvertenties op Telegram, platform laat handel ongemoeid*. <https://nos.nl/artikel/2506160-miljoenen-drugsadvertenties-op-telegram-platform-laat-handel-ongemoeid>
- Ouellet, M., Maimon, D., Howell, J. C., & Wu, Y. (2022). The Network of Online Stolen Data Markets: How Vendor Flows Connect Digital Marketplaces. *British Journal of Criminology*, 62(6), 1518–1536. Scopus. <https://doi.org/10.1093/bjc/azab116>
- Paquet-Clouston, M., & García, S. (2022). On the motivations and challenges of affiliates involved in cybercrime. *Trends in Organized Crime*. <https://doi.org/10.1007/s12117-022-09474-x>
- Politie. (2023, May 2). *288 aanhoudingen en €50,8 miljoen in beslag genomen bij internationale darkweb-actie*. Politie.NL. <https://www.politie.nl/nieuws/2023/mei/2/00-288-aanhoudingen-en-%E2%82%AC508-miljoen-in-beslag-genomen-bij-internationale-darkweb-actie.html>
- Politie. (2024, October 21). *Politie plaatst waarschuwingsbericht in Telegram-groepen na aanhoudingen datahandelaren*. <https://www.politie.nl/nieuws/2024/oktober/21/01.-politie-plaatst-waarschuwingsbericht-in-telegram-groepen-na-aanhoudingen-datahandelaren.html>
- Porter, K. (2018). Analyzing the DarkNetMarkets subreddit for evolutions of tools and trends using LDA topic modeling. *Proc. Digit. Forensic Res. Conf., DFRWS USA*, S87–S97. Scopus. <https://doi.org/10.1016/j.diin.2018.04.023>
- Pranckevičius, T., & Marcinkevičius, V. (2017). Comparison of Naive Bayes, Random Forest, Decision Tree, Support Vector Machines, and Logistic Regression Classifiers for Text Reviews Classification. *Baltic Journal of Modern Computing*, 5(2). <https://doi.org/10.22364/bjmc.2017.5.2.05>
- Radford, A., Kim, J. W., Xu, T., Brockman, G., McLeavey, C., & Sutskever, I. (2022). *Robust Speech Recognition via Large-Scale Weak Supervision* (arXiv:2212.04356). arXiv. <https://doi.org/10.48550/arXiv.2212.04356>

- Raman, R., Kumar Nair, V., Nedungadi, P., Ray, I., & Achuthan, K. (2023). Darkweb research: Past, present, and future trends and mapping to sustainable development goals. *Heliyon*, 9(11). Scopus.
<https://doi.org/10.1016/j.heliyon.2023.e22269>
- Röder, M., Both, A., & Hinneburg, A. (2015). Exploring the Space of Topic Coherence Measures. *Proceedings of the Eighth ACM International Conference on Web Search and Data Mining*, 399–408.
<https://doi.org/10.1145/2684822.2685324>
- Roks, R., & Monshouwer, N. (2020). F-gamers die ‘mapsen’, ‘swipen’ en ‘bonken’: Een netnografisch onderzoek naar fraude en oplichting op Telegram Messenger. *Justitiële Verkenningen*, 46(2), 44–58.
<https://doi.org/10.5553/JV/016758502020046002004>
- Roy, S. S., Vafa, E. P., Khanmohammadi, K., & Nilzadeh, S. (2024). *DarkGram: Exploring and Mitigating Cybercriminal content shared in Telegram channels* (arXiv:2409.14596; Version 1). arXiv.
<https://doi.org/10.48550/arXiv.2409.14596>
- Satrya, R. N., Pratiwi, O. N., Fa’rifah, R. Y., & Abawajy, J. (2022). Cryptocurrency Sentiment Analysis on the Twitter Platform Using Support Vector Machine (SVM) Algorithm. *2022 International Conference Advancement in Data Science, E-Learning and Information Systems (ICADEIS)*, 01–05.
<https://doi.org/10.1109/ICADEIS56544.2022.10037413>
- Schrama, V., van de Laarschot, J., Volten, C., & van Wegberg, R. (2022, November 8). *Virtuele Valuta—Handelingsperspectieven voor data-gedreven opsporing*.
<https://www.wodc.nl/actueel/nieuws/2022/11/08/bredere-blik-op-gebruik-virtuele-valuta-helpt-opsporing-criminele-gelden>
- scikit-learn. (n.d.). 1.4. *Support Vector Machines*. Scikit-Learn. Retrieved January 2, 2025, from <https://scikit-learn/stable/modules/svm.html>
- Sebastiani, F. (2002). Machine learning in automated text categorization. *ACM Computing Surveys*, 34(1), 1–47.
<https://doi.org/10.1145/505282.505283>
- Soska, K., & Christin, N. (2015). *Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem*. 33–48. <https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/soska>
- Statista. (2024, April). *Digital 2024: April Global Statshot Report*. Statista.
<https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/>
- Telegram. (n.d.-a). *Telegram Moderation Overview*. Telegram. Retrieved February 3, 2025, from <https://telegram.org/moderation?setln=en>
- Telegram. (n.d.-b). *Telegram Privacy Policy*. Telegram. Retrieved December 8, 2024, from <https://telegram.org/privacy/eu>
- Telemetr.io. (n.d.). *Analytics Service for Businesses on Telegram—Telemetr.io*. Retrieved December 8, 2024, from <https://telemetr.io/en>
- Uma, C., & Rathiga, P. (2024). An Optimized Deep Ensemble Super-Learner Model For Thyroid Disease Classification. *Library Progress International*, 44(3), Article 3.
- UNODC. (2024, October). *Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape*.
https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf
- U.S. Department of the Treasury. (2022, August 8). *U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash*. U.S. Department of the Treasury. <https://home.treasury.gov/news/press-releases/jy0916>

- Van Buskirk, J., Bruno, R., Dobbins, T., Breen, C., Burns, L., Naicker, S., & Roxburgh, A. (2017). The recovery of online drug markets following law enforcement and other disruptions. *Drug and Alcohol Dependence*, 173, 159–162. <https://doi.org/10.1016/j.drugalcdep.2017.01.004>
- Van Wegberg, R., Miedema, F., Akyazi, U., Noroozian, A., Klievink, B., & van Eeten, M. (2020). Go See a Specialist? Predicting Cybercrime Sales on Online Anonymous Markets from Vendor and Product Characteristics. *Proceedings of The Web Conference 2020*, 816–826. <https://doi.org/10.1145/3366423.3380162>
- Van Wegberg, R., Oerlemans, J.-J., & van Deventer, O. (2018). Bitcoin money laundering: Mixed results? *Journal of Financial Crime*, 25(2), 419–435. <https://doi.org/10.1108/JFC-11-2016-0067>
- Van Wegberg, R., Tajalizadehkhoob, S., Soska, K., Akyazi, U., Ganan, C. H., Klievink, B., Christin, N., & Eeten, M. van. (2018). *Plug and Prey? Measuring the Commoditization of Cybercrime via Online Anonymous Markets*. 1009–1026. <https://www.usenix.org/conference/usenixsecurity18/presentation/van-wegberg>
- Van Wegberg, R., & Verburgh, T. (2018). Lost in the Dream? Measuring the effects of Operation Bayonet on vendors migrating to Dream Market: WebSci'18. *Evolution of the Darknet Workshop at the Web Science Conference (WebSci 18)*, 1–5.
- Vana, P., & Pachigolla, P. (2021). *On the Deterrence Effect of Policing Anonymous Online Markets* (SSRN Scholarly Paper 3474719). Social Science Research Network. <https://doi.org/10.2139/ssrn.3474719>
- Verburgh, T., Smits, E., & Van Wegberg, R. (2018). Uit de schaduw: Perspectieven voor wetenschappelijk onderzoek naar dark markets. *Justitiële Verkenningen*, 44(5), 68–82. <https://doi.org/10.5553/JV/016758502018044005006>
- Wang, X., McCallum, A., & Wei, X. (2007). Topical N-Grams: Phrase and Topic Discovery, with an Application to Information Retrieval. *Seventh IEEE International Conference on Data Mining (ICDM 2007)*, 697–702. <https://doi.org/10.1109/ICDM.2007.86>
- Wang, Y., Arief, B., & Hernandez-Castro, J. (2023). Dark Ending: What Happens when a Dark Web Market Closes down. In Mori P., Lenzini G., & Furnell S. (Eds.), *Int. Conf. Inf. Syst. Secur. Priv.* (pp. 106–117). Science and Technology Publications, Lda; Scopus. <https://doi.org/10.5220/0011681600003405>
- Warner, C. (2023). Law Enforcement and Digital Policing of the Dark Web: An Assessment of the Technical, Ethical and Legal Issues. In *Applications for Artificial Intelligence and Digital Forensics in National Security: Vol. Part F1417* (pp. 105–115). Springer; Scopus. https://doi.org/10.1007/978-3-031-40118-3_7
- Wilson, T. J. (2020). Collaborative Justice and Harm Reduction in Cyberspace: Policing Indecent Child Images. *Journal of Criminal Law*, 84(5), 474–496. Scopus. <https://doi.org/10.1177/0022018320952560>
- Wokke, A. (2024, September 23). *Telegram gaat IP-adressen van verdachten op verzoek delen met autoriteiten*. Tweakers. <https://tweakers.net/nieuws/226882/telegram-gaat-ip-adressen-van-verdachten-op-verzoek-delen-met-autoriteiten.html>
- Yip, M., Shadbolt, N., & Webber, C. (2013). Why forums? An empirical analysis into the facilitating factors of carding forums. *Proc. Annu. ACM Web Sci. Conf., WebSci*, volume, 453–462. Scopus. <https://doi.org/10.1145/2464464.2464524>

Appendix A: Interview Protocol

*** The interviews were carried out in Dutch, this Protocol is therefore presented in Dutch ***

Opening:

- Kennismaking.
- Dit interview is onderdeel van een masterscriptie, het doel van het onderzoek is: De effectiviteit van toekomstige handhavingsacties verbeteren door empirische data te vergelijken met huidige perspectieven van inlichtings- en opsporingsdiensten en daarbij zowel operationele-, financiële- en gedragsperspectieven te gebruiken. De invloed van veranderende systeemkenmerken, zoals interventies, veranderingen op platforms en innovatie wordt hierbij onderzocht, in vergelijking met actueel gedrag in modi operandi in Nederlandse Telegram marktplaatsen.
- Dit interview duurt ongeveer 45 minuten.
- Dit interview wordt vertrouwelijk behandeld, wordt niet gedeeld en wordt verwijderd nadat het gesprek is samengevat. De enige andere personen die naar de opname van ons gesprek kunnen kijken, zijn mijn supervisors en mijzelf. Gaat u hiermee akkoord?
- Als we tijdens het interviewproces het risico lopen de scope te overschrijden, vind u het dan goed als ik de richting van het interview enigszins aanpas?
- Heeft u nog vragen voordat we verder gaan?

Interview:

Typen Criminaliteit en Aanpak

- Welke typen modi operandi komen veelvuldig voor op ondergrondse fora?
- Ziet u een verandering in de gebruikte modi operandi, in de afgelopen 5 jaar?

Betaalmethodes

- Welke typen betaalmethodes worden veelvuldig gebruikt?
- Ziet u een verandering in de gebruikte betaalmethodes, in de afgelopen 5 jaar?
- Ziet u een verband tussen de betaalmethode en de modi operandi?

Gedrag binnen Communities

- Kunt u beschrijven welke veranderingen u de afgelopen jaren hebt waargenomen in gebruikte betaalmethoden of de voorkomende modi operandi, naar aanleiding van interventies van opsporingsdiensten?
 - o Is dit gebeurd naar aanleiding van uitgevoerde of aangekondigde interventies?
 - o Heeft u specifieke voorbeelden van gevallen waarin criminele netwerken snel reageerden op interventies, en zo ja, hoe pasten ze zich aan?
- Kunt u beschrijven welke veranderingen u hebt waargenomen in de voorkomende modi operandi, naar aanleiding van technologische innovatie?
- Zijn er ook veranderingen waar te nemen naar aanleiding van platform veranderingen?
- Welke rol speelt de anonimiteit van platforms zoals Telegram of darknet-marktplaatsen in het vermogen van criminelen om hun gedrag aan te passen, en wat is de rol van veranderingen van anonimiteit (bijvoorbeeld zoals bij de Telegram case) op het vertoonde gedrag?
- Welke soorten fenomeenonderzoek verricht uw organisatie om veranderingen in crimineel gedrag op de langere termijn te identificeren?
- Hoe past uw organisatie haar aanpak aan wanneer criminelen zich richten op een andere modus operandi?

Appendix B: Telegram Market Descriptives

Table 7 presents the start and end dates for all scraped groups if this information could be derived from the data. It is possible that a group existed before the start of scraping (20-02-2021), which is denoted by a '<' symbol. Conversely, if a group did not cease operations prematurely (before 20-11-2024), this is indicated by a '>' symbol. However, this does not necessarily imply that the group is still active, as evidenced by groups 31 and 32, which were taken offline after the data collection. The precise reasons for this are unknown. In addition to these dates, data on the number of scraped messages, the count of unique authors, the total number of subscribers and the percentage of messages that have been forwarded from a broadcast channel have also been presented. Last, later in the analysis process (07-02-2025), it was verified whether the scraped channels were still operating, were held offline ('X') or were temporarily held offline ('T').

	Alias	Channel Opening	Channel Closure	Days Crawled	Number Messages*	% Broadcast	# Unique Authors	Offline (X)/Temp. (T)	Members/ Subscribers****
1	General_1	24-07-2021	>	1,215	16,881	94,9%	66		113
2	General_2	11-09-2024	12-09-2024	2	7	100,0%	2		12
3	General_3	20-02-2021	15-11-2024	1,364	923	9,0%	22		22
4	General_4	24-02-2024	08-03-2024	13	45,614	24,1%	182		1,802
5	Cars_1	<	>	1,369	12,559	0,0%	3,120		4,423
6	Cashout_1	29-02-2024	28-08-2024	181	28	100,0%	1	X**	925
7	Cashout_2	<	>	1,639	28,433	0,1%	350		246
8	General_5	10-11-2024	21-11-2024	11	52,189	42,0%	210		584
9	Cashout_3	16-7-2021	18-11-2024	1221	1,062	97,2%	27		27
10	Cashout_4	3-8-2021	24-6-2023	690	45	8,9%	12		7
11	Cashout_5	30-9-2024	15-11-2024	46	48	100,0%	1		295
12	General_6	<	19-11-2024	1,368	497	52,7%	39		24
13	Local_1	<	28-9-2022	585	65,652	38,3%	371		117
14	Drugs_1	5-10-2023	12-11-2024	404	18	100,0%	1		62
15	General_7	22-7-2021	18-11-2024	1,215	32	0,0%	6		8
16	Local_2	13-2-2022	>	1,011	5036	67,4%	120		129
17	General_8	25-2-2024	>	269	124,268	96,6%	587		667
18	General_9	10-8-2022	>	833	21,969	0,0%	6,852		16,997
19	General_10	6-1-2024	13-11-2024	312	10	100,0%	1	X	196
20	General_11	5-11-2024	>	15	129,077	52,3%	277	X	849
21	General_12	<	>	1,369	53,849	1,3%	573	X	1,916
22	General_13	6-11-2024	>	14	38,219	70,6%	135		2,196
23	General_14	16-3-2021	12-11-2024	1,337	178	29,8%	32		12
24	General_15	<	19-11-2024	1,368	180,024	5,1%	457		231
25	Local_3	18-7-2021	>	1,221	2,783	15,5%	140		106
26	General_16	<	>	1,369	215,805	1,4%	1,211		637
27	Local_4	27-1-2024	>	298	87	6,9%	26		63
28	Drugs_2	18-2-2022	9-10-2024	964	341	70,1%	2		5
29	General_17	26-4-2021	>	1,304	85,889	51,2%	314	T***	557
30	General_18	10-3-2021	17-11-2024	1,348	179	77,1%	10		18
31	Drugs_3	1-5-2024	1-5-2024	1	1	100,0%	1		45
32	Weapons_1	8-10-2024	17-11-2024	40	274	100,0%	1	X	1,118
33	General_19	6-11-2023	>	380	28	100,0%	1	X	Unknown

	Alias	Channel Opening	Channel Closure	Days Crawled	Number Messages*	% Broadcast	# Unique Authors	Offline (X)/ Temp. (T)	Members/ Subscribers****
34	General_20	<	>	1,369	74,410	46,9%	341		203
35	General_21	6-8-2021	1-12-2022	482	4	100,0%	1		475
36	Cashout_6	6-6-2024	16-9-2024	102	18	100,0%	1		127
37	Cashout_7	26-2-2022	14-2-2024	718	11	100,0%	1		181
38	General_22	<	>	1,369	20,759	74,1%	151		104
39	Local_5	11-11-2024	>	9	36,128	45,9%	386	X	2,654
40	Fireworks_1	10-10-2024	>	41	2,849	1,2%	436		1,373
41	Fireworks_2	<	14-11-2024	1,363	282	13,8%	57		121
42	Drugs_4	<	>	1,369	23,117	26,9%	893		4,742
43	General_23	16-6-2024	16-6-2024	1	2	100,0%	1		83
44	Local_6	14-4-2024	>	220	4,161	75,2%	60		112
45	General_24	26-10-2024	>	25	145,878	37,9%	255		574
Total:					1,389,624		14,856		

*Excluding blank messages (i.e. picture-only messages or voice memos), including potential duplicate messages

**This channel can't be displayed because it violated Telegram's Terms of Service'

****This group has been temporarily suspended to give its moderators time to clean up after users who posted illegal pornographic content. We will reopen the group as soon as it complies with the Telegram Terms of Service again.'

****Reference Date: 06-12-2024

Table 7: Telegram Channel Overview and Descriptives

Appendix C: Referenced Messages



**Although the formatting is identical to the actual message, blank lines have been removed*

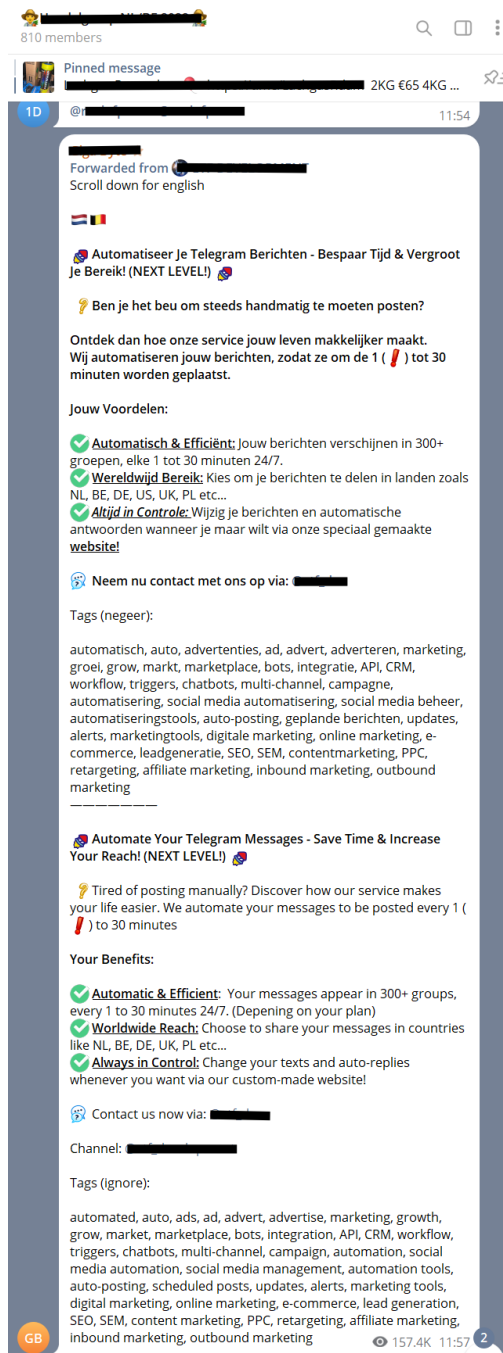





Figure 14: Message containing 'SEO tags'



JE KAART KAN MEE OP DE BOOT 🚢 🇪🇺

 ABN/ING/RABO/ASN/SNS/BUNQ/SKRIL
 BEL/ARG/BNP/AXA/KEY/KBC
 REAL/DZ/POST/BUND/BERG/LANDER/
 METRO/BARC/HBOS/HSBC/ROYAL

(alle kaarten zijn welkom)

Belangrijk: kaarten moeten compleet ingeleverd worden met internetbankieren en code. Wij accepteren geen kaarten onder bewind, de kaart mag in zijn geheel leeg zijn. Er hoeft dus geen saldo op te staan. Je kaart moet geactiveerd zijn en niet geblokkeerd! Stel de opnamen limieten in op zijn maximale zodat, we het maximale er uit kunnen halen. Heb je een kaart van 18- word die ook geaccepteerd zo lang het maar compleet is.

Percentage is 45 tot 50%. Er wordt op afstand gewerkt op het moment dat er op langer termijn wordt samen gewerkt. Alles wordt samen gepind.

Figure 15: Request Message for Money Mules

Appendix D: Confusion Matrices

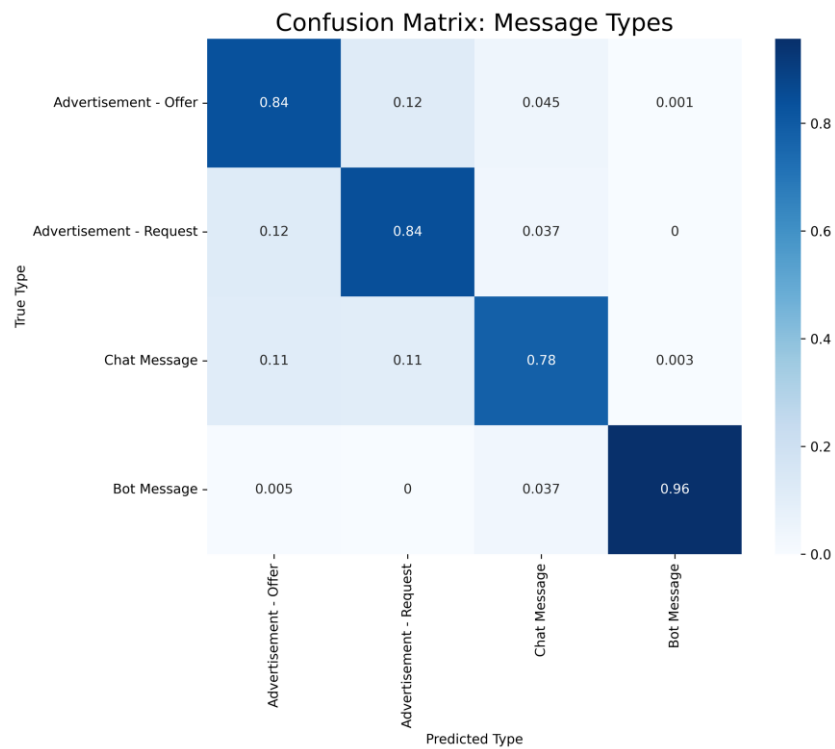


Figure 16: Message Types Confusion Matrix

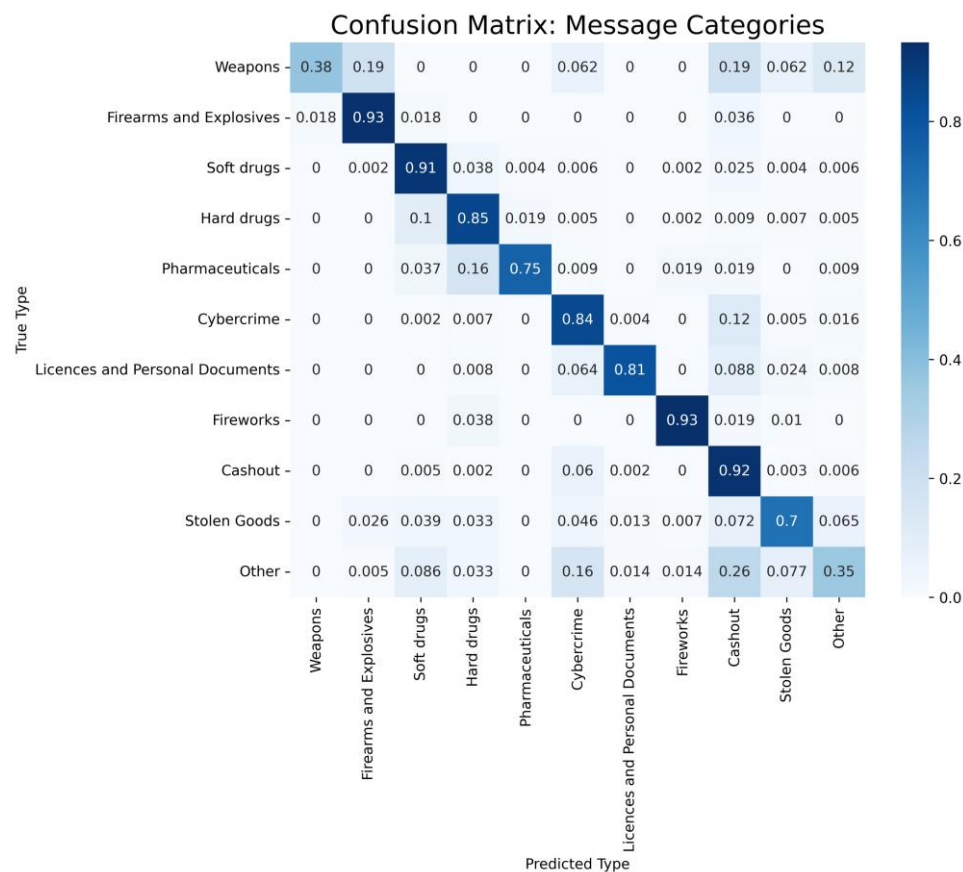


Figure 17: Advertisement Category Confusion Matrix

Appendix E: LDA Addendum

This Appendix provides the labels associated with the latent topics identified through the LDA analyses. Sections E.1 and E.2 show the word-weight combination for the analyses conducted on chat messages and bot messages, respectively. The messages have undergone preprocessing, making them moderately cryptic and lacking words that were filtered out earlier. Words with an underscore ('_') indicate that they have been combined during the creation of bigrams and trigrams, as they frequently co-occur. Section E.3 presents the full analysis of chat messages using the reference dataset (2017 to 2021).

E.1 Chat Messages: Topic Words



Figure 18: Chat Message Topics

Several topics have not been presented in earlier chapters. For full transparency, they will be elaborated upon:

- The first topic highlights discussions about automated advertising and e-commerce bots that automatically send or forward advertisements across various channels. Terms such as *'groei begint vandaag'* (translation: *'growth starts today'*), *'automatisch'* (*'automatic'*) and *'winkelstof'* (*'shop bot'*) indicate discussions about the exchange of services in which users outsource part of their supply chain.
- The second and third topic do not effectively classify as chat messages, which may be attributed to several factors. The second topic consists primarily of a compilation of German words that appear frequently within the current dataset. Terms such as *'fuhrerschein'* and *'prufungen'* (driver licences and fake test results) indicate the presence of (German) documents that have not been categorised under *'Ad. – Offer'* and *'Licences & Personal Documents'*, demonstrating that criminals operate across borders. The third topic represents multiple subjects, which is an example of the overfitting nature of the model. On one hand, there is communication around *'OnlyFans'*, *'online rooms'*, *'TikTok'*, and prostitution. On the other hand, discussions arise regarding (luxury) taxis, including or excluding taxi board computers.
- Topics 5, 6, 7 and 9 focus on the discussions around specific products. In the fifth topic, various kinds of drugs are discussed, and new channels where drugs are openly exchanged are sent with their Telegram URL in this topic. Posts are often sent with pictures of the available goods, which is indicated by the word *'zien'*. A manual search through the messages has confirmed that these chat messages are often accompanied by pictures of vast volumes of drugs (such as full blocks of cocaine or heroin), showcasing that the vendors are theoretically able to deliver the offered products. Topics 6 and 7 mainly mention perfumes in original packages (with photos of the fake boxes with legitimate barcodes which appear legitimate as a result) and fat burners and weight loss supplements, such as *'iomax'*. Topic 9 discusses the sale of (illegal) fireworks. The various types of fireworks (e.g. *'dumbum'*, *'shell inch'* and *'enigma'*), familiar vendors, and the methods of delivery or collection are hereby discussed.

When comparing the found latent topics in chat messages from the current (this section) and reference dataset (Appendix E.3), latent topics are witnessed that were not present in both timespans. Specifically, the reference dataset highlights conversations about renting 'panels', scamming stories for fellow Telegram users, recruitment efforts for 'soldiers' or 'workers' (money mules) willing to provide their credentials for cash-out fraud (closely overlapping offer advertisement offer) and proof of delivery for illicit products. While these topics did not emerge in the results of the current LDA analysis, similar chat messages were identified but did not yield an individual latent LDA topic. In contrast, the current dataset contains more discussions focused on individual products and their usage (topics 5, 6, 7 and 9).

E.2 Bot Messages: Topic Words

Below, the word-weight combinations for the bot messages are presented. Hereby, only messages used to inform, warn, or automatically ban users are incorporated. A significant number of bot messages are also used to forward advertisements or messages across multiple channels, but these were not included in this dataset, as they did not receive 'Bot Message' as message type label.

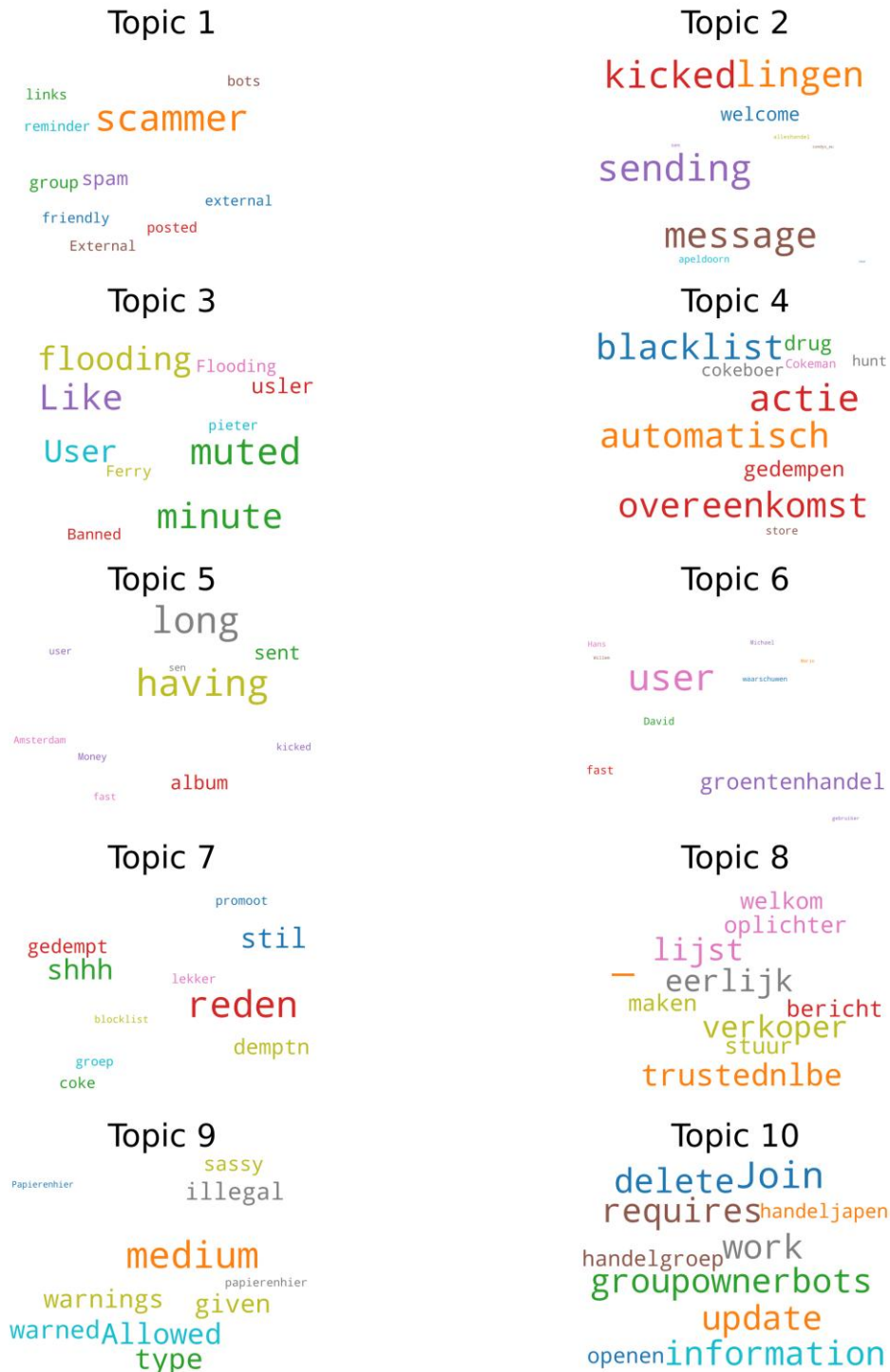


Figure 19: Bot Message Topics

E.3 (Reference Dataset) Chat Messages: Full Analysis

The reference (*'Virtuele Valuta'*) dataset comprised a total of 1,236,129 chat messages collected from Telegram, from 2017 to 2021. After preprocessing the data following the steps outlined in Subchapter 6.3, 557,301 messages remained for analysis, containing 53,307 unique tokens. Figure 20 presents an overview of the found coherence scores over the number of latent topics. The results indicated that the optimal model emerged with five latent topics, achieving the highest coherence score of 0.532.

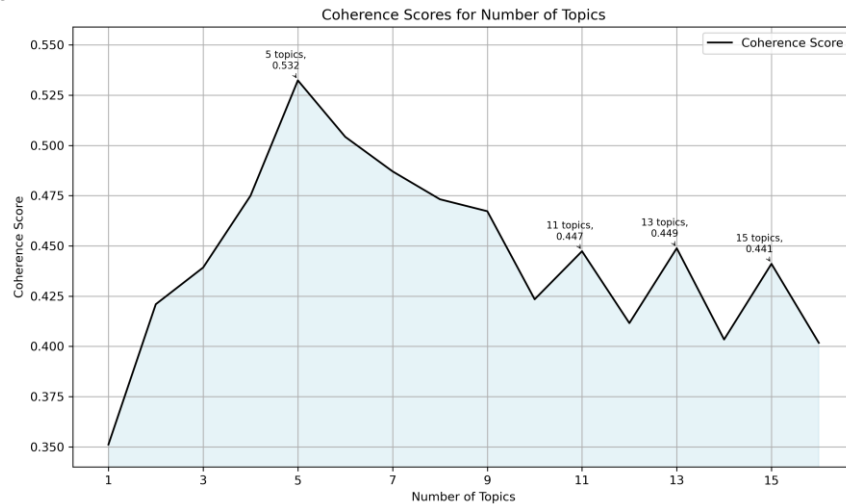


Figure 20: Coherence Scores for Reference Dataset (2017-2021)

From the five latent topics identified, word clouds have been created based on the identified word-weight combinations and their internal probability, as presented in Figure 21. The word-weight combinations and the exported grouped messages were reviewed, leading to the identification of the following five topics:

1. **'Bonken', 'Soldiers', Panels & Cash-Out Discussions.** 'Bonkers' are individuals who have gained access to online banking details (such as usernames and passwords) and need methods to transform digital currencies into cash, often using money mules. The first latent topic discusses the 'rental' possibilities of the pages utilised for extracting that data (including fraudulent payment request pages or banking login pages), along with all practical considerations associated with their usage. 'Soldiers' are then sought, as can be seen in Figure 15 in Appendix C. Fraudulent transactions are then made to their IBAN accounts, and the funds are withdrawn as cash from ATMs, effectively converting stolen money into fiat currency. This method of cash-out is extremely prevalent, which is also witnessed in the high volume of cash-out advertisements observed in the current dataset. These advertisements further reveal a disregard for ethical boundaries, as no hesitation in targeting vulnerable groups, including minors and, in some cases, individuals under financial guardianship, is displayed. Key terms relevant to this topic include: *'bonkpanels'*, *'betaalverzoek'*, *'custom'*, *'verhuur'*, *'ingbanknl'*, *'abnbanknl'*, *'hetbureau'*, *'rabobanknl'*.
2. **Recommendation of other Telegram Channels.** This topic has strong similarities with the fourth identified topic from Chapter 7.1.3, where users are encouraged to join other channels in various types of criminal activities. Examples here include drug and arms trafficking, as well as the trade of leads and accounts and even clothing, with their corresponding invitation link.
3. **Alerts for Scammers.** Similar to the 8th and 10th latent topics found in the LDA model with chat messages from the current dataset. Warning and informing users of potential scammers (unfair prices, low-quality products, and *'infotrekkers'*).
4. **Scamming Stories & Workers Recruitment.** Occasionally, chat messages are shared, often lengthy texts, that closely resemble 'Nigerian Prince' emails. In these messages, an individual claims to have been helped by someone and to have made large sums of money as a result. These messages aim to tempt others into a

trap to extract money, often through schemes such as pig-butcher or fraud, promising ‘massive payments.’ Within the same category are messages from people seeking ‘workers’, namely individuals willing to provide their bank credentials in exchange for large sums of money, enabling others to perform cash-outs. These individuals are often referred to as ‘soldiers’ in the chat channels, with phrases like ‘soldaten erin, ratten wegblijven’ (‘soldiers in, rats stay out’) commonly used to lure new individuals.

5. **Proof of Delivery or Services.** In contrast to the third topic, there are also messages where recipients express satisfaction or their gratitude with the delivered services or products. In these cases, a vendor or product has proven reliable, and recipients share photos of the received items as proof in the channel or post a thank-you message, sometimes showing non-standard delivery times (e.g. late at night). The length of these messages varies significantly. Common goods mentioned in these messages include firearms or delivered bank panels.



Figure 21: Chat Message Topics (2017-2021)

Appendix F: Payment Methods Addendum

This appendix has a two-fold function. Appendix F.1 functions as a supplement to Chapter 6.4. The second part, F.2, presents the full results of the analysis.

F.1 Addendum to Chapter 6.4 (Approach)

In Figure 22, signal words are incrementally added, showing a decline in missed payment indicator words until saturation is reached, indicating that the list with signal words is complete. Table 8 displays the list of payment indicators that were utilised and those that were excluded.

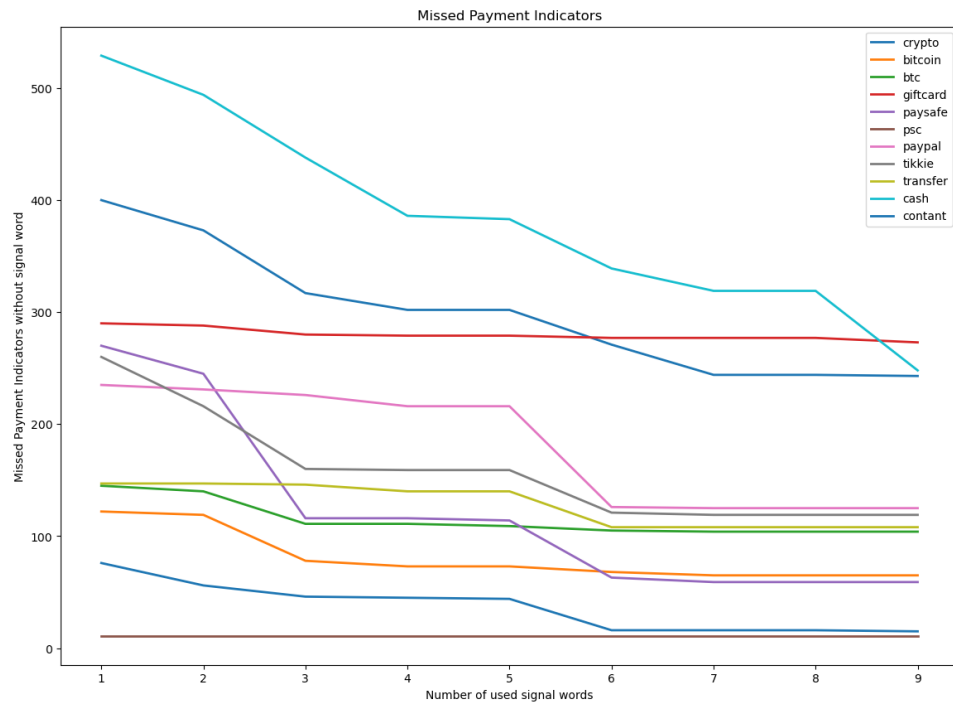


Figure 22: Missed Payment Indicators per Added Signal Word

Type	Indicator	Remark
Cryptocurrencies	crypto	Added: Frequently utilised as a substitute for terms as 'bitcoin' or 'btc'
	bitcoin	
	btc	Added: Often used abbreviation for 'bitcoin'
	xbt	Removed: Occurs infrequent and too frequently encountered with other purpose rather than as a payment method
Giftcards	giftcard	
PayPal	paypal	
	paypal	Removed: Too similar to 'paypal', results in duplicates.
	pp	Removed: Occurs often, too frequently encountered with other purpose rather than as a payment method
PaySafeCard	paysafe	
	paysafecard	Removed: Too similar to 'paysafe', results in duplicates.
	psc	Added: Often used abbreviation for 'psc'
Transfers & 'Tikkie'	tikkie	
	transfer	Added: Often used besides 'Tikkie'
Cash Payments	cash	
	contant	
	contante	Removed: Too similar to 'contante', results in duplicates.

Table 8: Currencies Wordlist

F.2 Preferred Payment Methods

This chapter draws on offer advertisements to provide an overview of the payment preferences that vendors communicate to potential buyers. By examining these preferences, it becomes possible to link specific types of criminal activity to particular payment methods. In addition, the chapter investigates whether single-category vendors and multi-category vendors show different payment requirements, potentially indicating the degree to which these vendors specialise within a certain domain. Following the approach outlined in Chapter 6.4, various insights can be derived. It was found that cash payments are strongly preferred in absolute numbers, while cryptocurrencies (e.g. 'crypto,' 'bitcoin,' and 'btc') are also frequently requested as the preferred method. To provide insight into preferred payment methods by advertisement category, this distribution has been plotted in Figure 23.

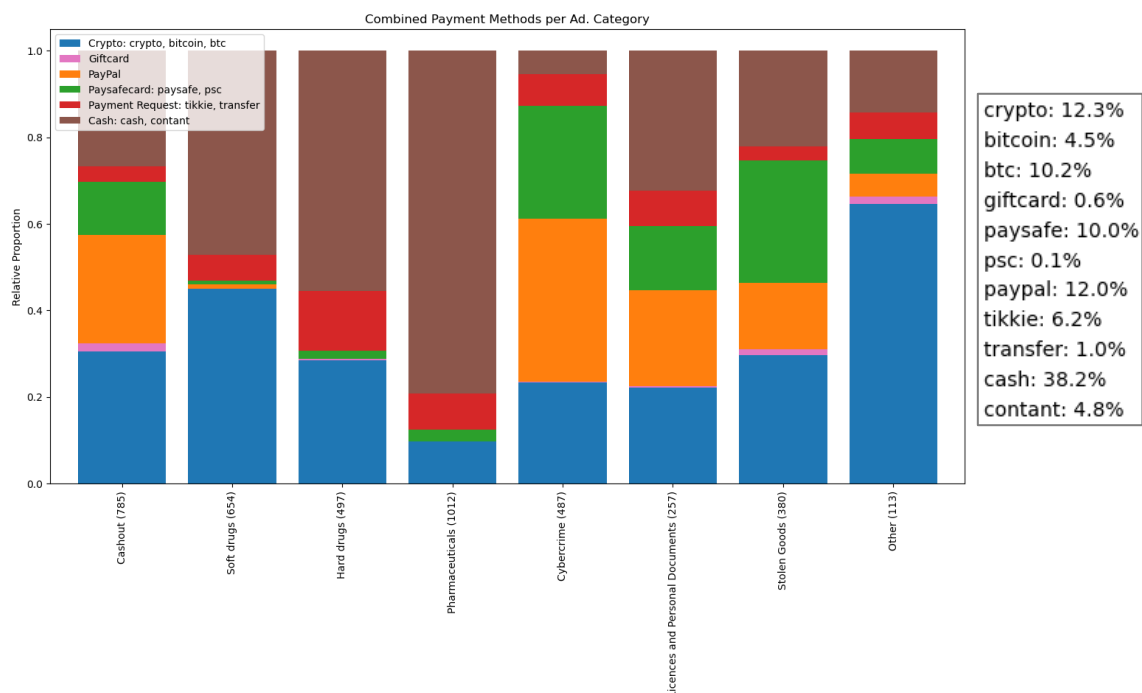


Figure 23: Payment Preference per Ad. Category and Overall Distribution

It only displays eight categories, while eleven categories were manually labelled for. This is because categories 'weapons', 'firearms and explosives' and 'fireworks' only had respectively 9, 7 and 9 ads where the preferred payment method was specified. If these were displayed, data could be misinterpreted more easily. To get a better understanding of the relationship between the ad categories and preferred payment methods, a heatmap (correlation matrix) was crafted, as shown in Figure 24.

The scraped messages provide only a snapshot of the collection period, as the majority of messages originate from the last two weeks of the dataset. This makes it challenging to identify changes over the scraped years. However, it is possible to compare these results with earlier insights from the reference dataset. Therefore, the analysis was performed a second time. The results of the reference analysis are presented in Figure 25.

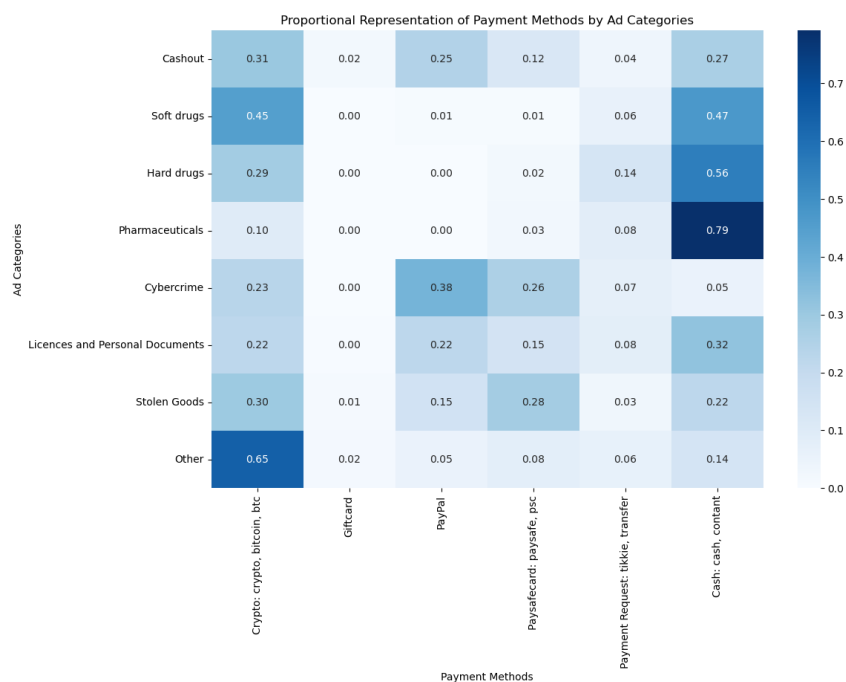


Figure 24: Heatmap: Relation between Ad. Category and Preferred Payment Method



Figure 25: Heatmap: Relation between Ad. Category and Preferred Payment Method (2017-2021)

Based on the two heatmaps and Figure 23, various key insights can be derived:

- **Shift from Cryptocurrencies to Cash in Drug-Related Categories.** Payment preferences in Soft drugs, Hard drugs, and Pharmaceuticals have shifted significantly from cryptocurrency to cash. Soft drugs (47%), Hard drugs (55%), and Pharmaceuticals (79%) show a clear reliance on cash, reflecting the preference for direct, untraceable exchanges, especially for physical goods. The exact reason for the high correlation between these individual crime types and cash is not empirically determinable, but this could be due to the physical nature of these transactions, in combination with the pre-existing in-person contact, making cash the preferred option. However, this trend is not reflected in the use of digital payment requests, such as 'tikkie'.
- **General Decline in Use of Tikkie and Bank Transfers.** There has been a noticeable decrease in the use of legitimate payment methods like Tikkie and bank transfers for illicit transactions (except for the hard

drug category). This could be due to the growing reluctance to use methods tied to identifiable personal information such as names and addresses. There is an increased interest in anonymous methods like Paysafecard at the same time, which offers better privacy and security for illegal transactions as it is more anonymous.

- **Digital Payment Options for Financial- and Cybercrime.** Paypal has become the dominant choice in Cybercrime (38%), followed by Paysafecard and cryptocurrencies. As PayPal only requires a name, address, phone number and email address, which could all be falsified, it provides similar privacy to Paysafe and cryptocurrencies. Their prevalence could also be due to the inherently online nature of cybercrime activities. A similar pattern is observed in cash-out advertisements, where illegally obtained funds are laundered into fiat currency. Digital payment methods are prevalent in this category, as these are often used for such transactions. Additionally, cash also plays an important role, particularly in cases involving counterfeit bills, which are sold in exchange for genuine currency, driving the demand for cash.
- **Cryptocurrencies in the 'Other' Category.** Last, in the 'Other' category, a spike can be witnessed in the use of cryptocurrencies. Cryptocurrencies account for a large proportion (65%), which could be largely attributed to their use in activities such as sports betting on fixed matches, particularly in regions like Africa.

F.3 Preferences for Single- vs Multi-Category Vendors

In Chapter 7.4, it was determined that 32.4% of vendors offer multiple categories of crime. While Appendix F.2 examined the relationship between individual crime categories and payment methods, this does not address the decision-making of multi-category vendors. The question arises whether offering multiple types of illicit goods or services also leads to accepting a wider range of payment methods. To investigate this, the average number of payment methods was calculated for both single- and multi-category vendors. Since vendors typically do not use multiple indicative terms for the same payment method (e.g. 'BTC' and 'Bitcoin') in the same sentence, this metric reflects the number of distinct payment methods accepted. The findings reveal that, among vendors specifying a payment method, single-category vendors accept an average of 1.37 payment methods, while multi-category vendors accept an average of 1.63 payment methods throughout their advertisements.

These values have been calculated based on 620 unique single-category vendors and 131 multi-category vendors, indicating that the number of vendors specifying a particular payment method is relatively low. Furthermore, most vendors have multiple listings per individual with the same payment preference, as they prefer to be paid in this manner. Figure 26 illustrates the distribution of the number of payment methods specified across all advertisements for both single-category and multi-category vendors.

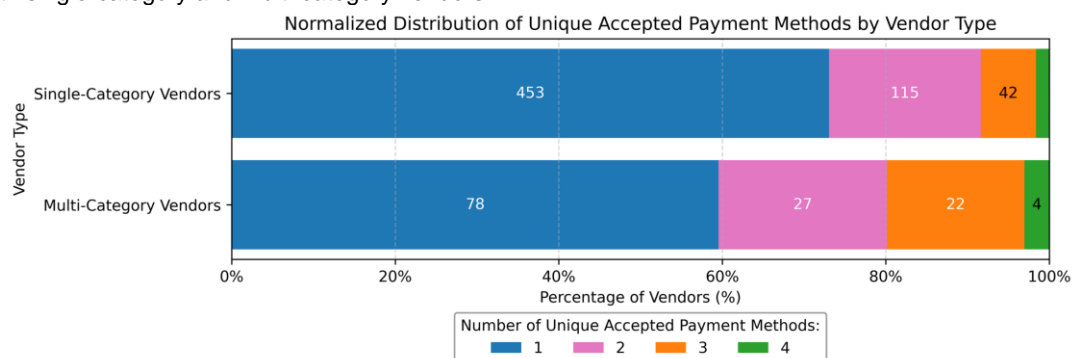


Figure 26: Uniquely Accepted Payment Methods per Vendor Type

This analysis has proven that multi-category vendors, on average, accept slightly more payment methods than single-category vendors; however, this difference is minimal. To assess whether this difference is statistically significant, a Welch's t-test (that adjusts for both unequal variances and unequal sample sizes) was conducted, which yielded a t-statistic of (-)3.27, indicating that single-category vendors have, on average, fewer unique payment methods than their multi-category counterparts. With a p-value of 0.0013, this difference is statistically significant, suggesting that vendors offering multiple categories of illicit goods or services are more likely to diversify their payment options.