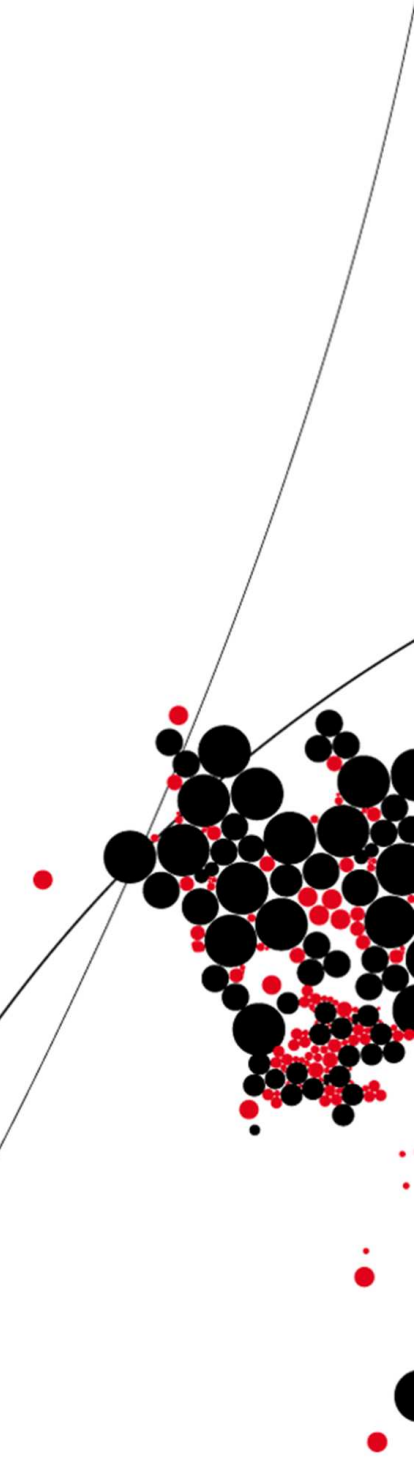
UNIVERSITY OF TWENTE.

Faculty of Electrical Engineering, Mathematics & Computer Science

Is Telegram the new Darknet? A comparison of traditional and emerging digital criminal marketplaces

D.L.M. Lummen

M.Sc. Thesis
March 2023



Supervisors:
Dr. Anna Sperotto
A. Vogelaar

Committee Members:
Dr. Andrea Continella

Faculty of Electrical Engineering,
Mathematics and Computer Science
University of Twente
P.O. Box 217
7500 AE Enschede
The Netherlands

Abstract

Digital criminal marketplaces on the Darknet have existed for many years, giving users the opportunity to buy and sell a large variety of illegal goods and services. Law enforcement has had an increased focus in taking down these Darknet marketplaces in the last years. At the same time, a new type of digital criminal marketplace has risen on the messaging app Telegram. In this research the differences and similarities between the two types of criminal marketplaces are evaluated in terms of organisational structure, users, goods and services advertised and their development over time. In general, Telegram marketplaces are easier to use. However, for this ease of use users compromise by not having access to systems that can protect both buyer and seller in the ordering process, which Darknet marketplaces do have.

Contents

Chapter 1

Introduction

Online criminal marketplaces have already existed for many years, mainly in the shape of marketplaces on the so-called darknet. Darknets are overlay networks within the dark web (the non-indexed part of the Internet) that are only accessible via specialised anonymity software such as Tor. These criminal marketplaces are used for the buying and selling of a large range of goods and services: from illegal drugs and toxic chemicals to counterfeit goods, malware and firearms. Over the years, law enforcement have investigated and seized numerous different darknet marketplaces, after which new marketplaces are set up and the cycle repeats itself. One of the main reasons why these criminal marketplaces thrive on the darknet is due to the ability for people to be anonymous. In recent years, criminals have started using the messaging app Telegram to host marketplaces in channels and groups as well. This is because Telegram is widely promoted as a messaging app where the privacy of messages and users is the number one goal, and a lot less technical skill is typically needed to use a messaging app on a phone than to access a marketplace on the darknet. Our intuition is that there might be some interesting similarities and differences between the marketplaces on the darknet and those on Telegram. Therefore, this research tries to discern the differences and similarities of these upcoming markets on Telegram in relation to the markets on the darknet.

1.1 Motivation

A lot of research has already been done on cybercrime on darknet marketplaces and forums as well as in Telegram chat groups. However, not much research has been done to the possible connection as well as differences and similarities between

the two. Besides, there is currently also little to no literature about this topic. The possibility exists that criminals use both platforms and that the services and goods they provide are available in multiple different places. However, it could also be the case there is no overlap and that there is a clear distinction in the criminals providing goods and services on the darknet versus those providing goods and services through Telegram. Given the major law enforcement action taken towards marketplaces on the Darknet there could be a shift from the relatively tech savvy darknet marketplaces towards a more simplistic platform such as Telegram. The overall goal of this research is to characterise the upcoming markets on Telegram and their relation to those on the darknet.

1.2 Research Questions

To investigate the characteristics, overlap and connection between the two types of marketplaces we therefore define a number of research questions. The main research question being:

MQ What are the differences and similarities between traditional digital criminal marketplaces and emerging criminal marketplaces on Telegram?

To answer this main research question, we will answer the following sub-questions:

SQ1 What are the differences in organisational structure between traditional digital criminal marketplaces and emerging digital marketplaces on Telegram?

SQ2 How do users engage with the different types of marketplaces?

SQ3 What are the differences in types of goods and services being advertised on traditional criminal marketplaces and emerging digital criminal marketplaces on Telegram?

SQ4 How is the usage of both traditional criminal marketplaces and emerging digital criminal marketplaces on Telegram developing over time?

For **SQ1**, we want to look at the organisational structure of the marketplaces in the sense of how these marketplaces are run and how they are managed. We will research if the marketplaces are being run by a single person or by a group. We will also look at if there are any moderators that are monitoring the marketplace or if

there are any other systems in place, such as bots, to help run the marketplace. The payment methods for the different types of marketplaces will also be compared.

For **SQ2**, we focus on the users of the criminal marketplaces and how they use the different marketplaces. We will compare the users on Telegram with those on the Darknet marketplaces in terms of total number of users and number of active users. A comparison will also be made between the amount of users selling goods and services versus the amount of users buying goods and services on each of the marketplaces.

SQ3 will be answered by looking at the specific goods and services provided on the different marketplaces. We will look at the total amount of goods and services advertised on each of the marketplaces, while also specifically looking at the goods and services shipping from the Netherlands. Secondly, we will look at the different categories of goods and services that are advertised and a comparison will be made between the different marketplaces. Finally, the advertisement messages will be compared to see if there are specific ways of advertising related to a marketplace.

To answer **SQ4**, we will look at the development of the marketplaces over time. The number of users over time as well as the number of active users will be compared between the two types of marketplaces to see if the markets are still growing or if there is actually a decrease in growth. In order to do this, a timeline will be created. Next to this, an overview will be made between the number of messages/activity per day over a period of time to get an accurate view of the usage of the marketplace.

1.3 Overview

Chapter 2 provides background information on both the darknet and the marketplaces it hosts as well as on the Telegram application. Related work to the current research can be found in Chapter 3. The two datasets used in the research will be discussed in Chapter 4, whilst the methodology used to answer the research questions can be found in Chapter 5. Chapters 6, 7, 8 and 9 provide the results for each of the four sub research questions respectively. Finally, conclusions, a discussion of the results and proposed future work can be found in Chapter 10.

Chapter 2

Background Research

In the following Chapter, an elaborate background is given on both the darknet and darknet marketplaces/forums as well as Telegram and its marketplace groups.

2.1 Deep Web, Dark Web & Darknets

There are numerous terms that are used to refer to different parts of the web, which can be explained with the analogy of an iceberg floating in the water, as shown in Figure 2.1. The 'surface web' corresponds to roughly 10% of web pages on the web [1]. These are the web pages that are indexed and can be found using regular search engines such as Yahoo and Google. All other web pages are classified as 'deep web'. The deep web consists of all pages that are not indexed and cannot be accessed through search engines. They are however, accessible through a specific URL address. In the news, the deep web is often used as a term for the web where illegal activity takes place. However, a large portion of these web pages is benign. For example, if an article online is only able to be read with a subscription to the website, this page cannot be indexed by a crawler and therefore is part of the deep web [2]. Another example are the web pages one accesses when doing any kind of online banking, as these are locked behind a log-in form. In conclusion, deep web pages can be concealed behind passwords, or can tell search engines not to index them.

A small portion of the deep web is called the 'dark web'. This dark web content exists on darknets. Darknets are overlay networks within the web that are only accessible via specialised anonymity software such as Tor or I2P [3]. The terms dark web and

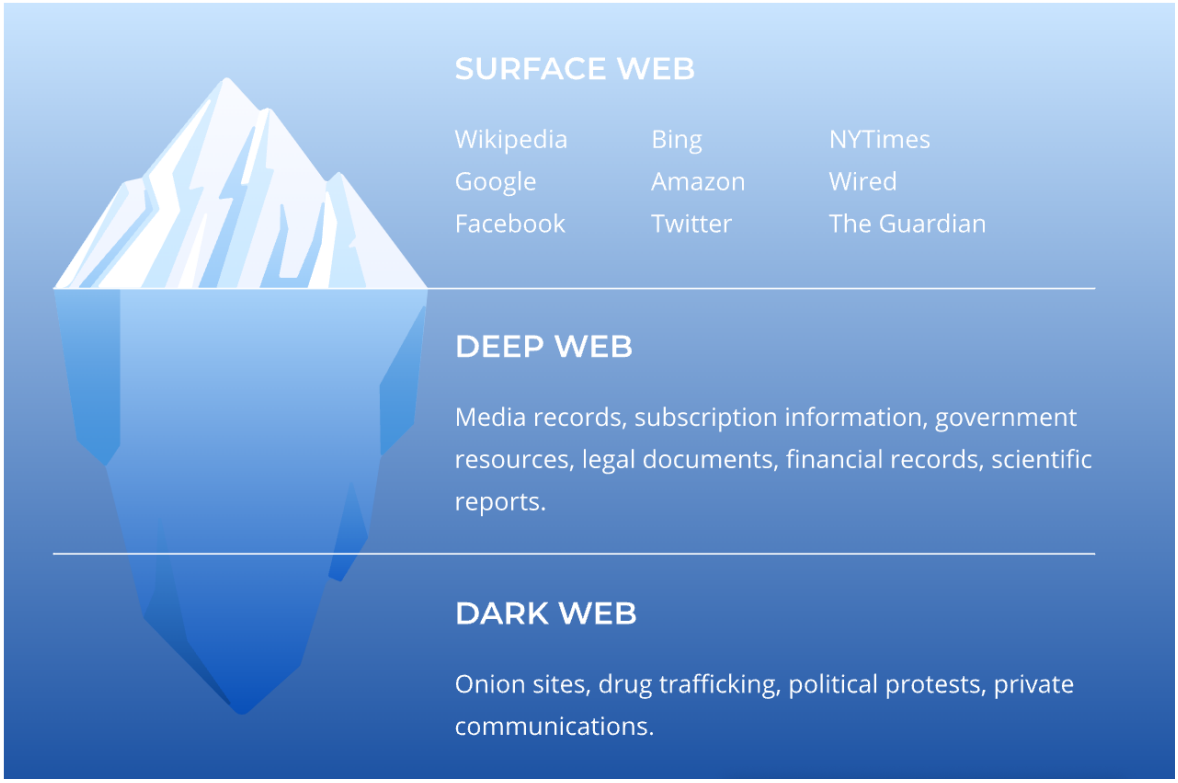


Figure 2.1: Surface web, Deep web and Dark web [4]

darknet are often used interchangeably in both the media and research, mainly due to the fact that a very large portion of the dark web is located on Tor's darknet. Most darknets are initially developed with good in mind, such as improved anonymity, and can have many positive uses as well. Darknets for example, allow the escape of censorship for journalists in countries with limited free speech. However, this increased anonymity also attracts negative uses and abuse. The darknet is therefore also used for a lot of criminal activities, with many darknet marketplaces emerging providing illegal goods and services.

2.2 Darknets

There are a number of different darknets out there, with TOR being the biggest and most well-known. In the following section we will discuss the three most common darknets: TOR, I2P and Freenet.

2.2.1 TOR

The most well known darknet in the world is called TOR, short for The Onion Router. One of the main advantages TOR has is the fact that it has its own designated TOR browser [5]. The goal of Tor is not to completely stop tracking, but to reduce the likelihood of sites tracing actions and data back to specific users. It uses an implementation of onion routing, which provides anonymous connections that are resistant to eavesdropping and traffic analysis [6]. The main idea behind onion routing is that a message is wrapped by a number of layers of encryption, like layers of an onion. Tor uses a global overlay network of relays. A number of successive relays (with a minimum of three relays) is used as the virtual route for the message to traverse. At the source, the message is encrypted with the encryption key for each relay node of the path it needs to traverse to reach the destination. The most outer layer of encryption is decrypted by the entry node in the network, whilst the most inner layer of encryption is decrypted by the exit node in the path. This way each relay node only gets the address of the next hop in the route and therefore do not know then entire route. At the exit node the final layer of encryption is decrypted and the message is forwarded to its final destination [7].

2.2.2 I2P

The Invisible Internet Project, or I2P, is next to TOR the most commonly used Anonymous Communication Network. However, the two work slightly different. Where Tor is an overlay network, I2P is an overlapping network based on 'garlic routing'. Cells contain the encrypted payload of the message as well as the instructions to other onion router nodes. Onion routing uses cells of a fixed size as to avoid fingerprinting and attacks against a specific sender or receiver. However, these fixed-size cells pose a vulnerability against man-in-the-middle attacks and replay attacks due to the absence of randomised data padding and intentionally introduced delays [8]. Garlic routing is similar to onion routing, but an extra step is added. Instead of onion cells, garlic routing uses garlic cloves. A garlic clove is a number of onion cells that are grouped together and padded with random data. A delay or no-delay instruction is also added to the garlic clove so other I2P nodes know if a garlic clove needs to be delayed at that node. To add even more randomness the number of onion cells per garlic clove differs between the I2P nodes. When an I2P node receives a new garlic clove, it can decrypt it and then use each onion cell independently as it would in onion routing. If it needs to send the cells to another I2P node it creates a new garlic clove like described above. [9]

2.2.3 Freenet

Freenet is an overlay peer-to-peer network, therefore each computer in the network is responsible for a portion of the tasks on the network. Next to this, a machine in the Freenet network also stores files that are available for all Freenet users. The two main differences between Freenet and TOR are that TOR uses a client-server model which has a single source for a specific web page or certain data. Freenet uses a distributed model, with files and pages that are located on a number of different machines of Freenet users. This makes Freenet more resilient against takedowns, but the limitation of this distributed setup is that the speed is slower. Secondly, TOR allows users to also browse the surface web, whilst Freenet is its own closed off network [10]. Documents are stored on the Freenet network by using a specific unique key, which consists of a binary string. This key is used to decide where the document is stored in the network as well as to prove authenticity when the document is transfered [11].

2.3 Darknet Markets

Whilst there are a lot of legitimate uses for using darknets, for example to ensure the privacy of journalists in countries with limited free speech, darknets are also often used for illicit purposes. Example of these illicit purposes are the illegal trade in narcotics, counterfeit documents, weapons and other services. These marketplaces are built on the darknet as to provide as much privacy for their users as possible.

2.3.1 Darknet Markets Structure

Visually, darknet marketplaces are very similar to popular surface web marketplaces such as Amazon and eBay. There are different categories for the different types of products being sold such as drugs, services, counterfeits etc. An image of the homepage of the AlphaBay darknet marketplace can be seen in Figure 2.2. There are two types of users on these markets, buyers and vendors.

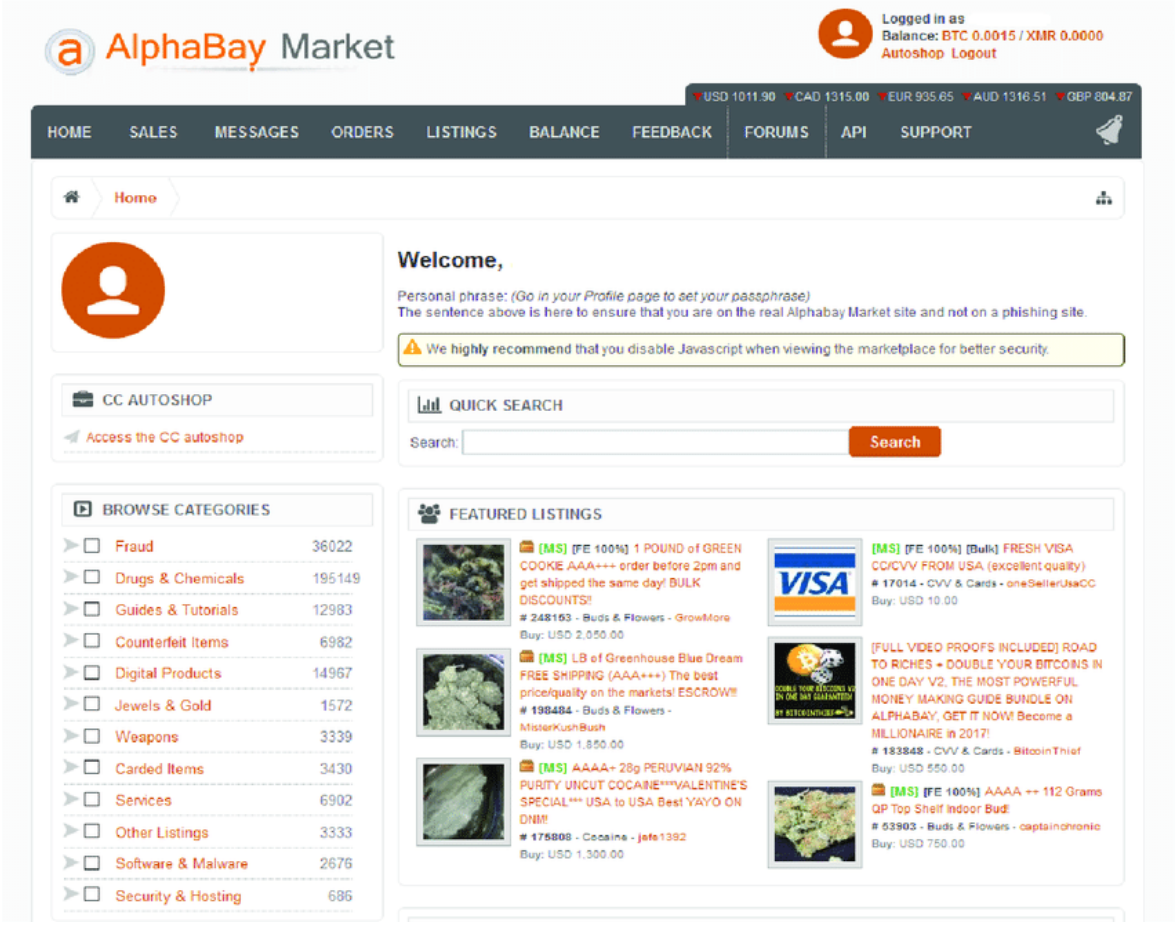


Figure 2.2: AlphaBay homepage [12]

Vendors

Before vendors are able to advertise and sell their products on the marketplace, they first have to set up their specific store on the marketplace. In order to do this, vendors have to pay a vendor fee to the market, which differs from market to market. Next, vendors can provide information on their products, shipping, bulk discounts etc. Vendors try to create a brand identity to invite users to buy their products, similarly to how this is done on surface web marketplaces [13]. Most marketplaces also charge a sales commission which varies by the type of product being sold, for example on the Hydra marketplace this was generally 5% of the purchase price [14].

Buyers

Users are able to create accounts and communicate with vendors using private messaging. In the case that the user wants to buy an item they have to prepare for the delivery of the item, such as by deciding if it needs to be shipped to a separate post box or to their homes, and have the appropriate funds in cryptocurrency in their wallets on the marketplace. Section 2.3.2 goes into more detail on the payment process.

Most marketplaces rely heavily on trust, therefore rating and review systems play a large role in the sale of goods. This review system is a big aid in informing customers on the reputable vendors on the marketplace and helps avoid scam sales. Customers are usually asked to leave a review describing the quality of the product and the ordering process as well as rating the vendor on a scale of 1 to 5 [15]. Next to the owners of the marketplace, the day-to-day business is run using moderators who take on all support questions and dispute handling on the marketplace. The group of moderators can be relatively small, but can also be very large with moderators only having a very specific singular task (such as keeping up a server).

2.3.2 Payment

Most transactions on darknet markets are done through digital wallets on the marketplace, in which users can deposit digital coins of different cryptocurrencies. The most accepted cryptocurrencies are Bitcoin (BTC), Bitcoin Cash (BCH), Ethereum (EHT) or Monero (XMR) [16]. Almost all markets also make use of an escrow system to protect both the buyer and seller of goods. Payment for the goods is sent from

the buyer to the market, which holds it in an escrow account until the order arrives and the buyer can finalize the transaction. This authorises the market to release the money held in escrow to the seller. Should the buyer not be satisfied with the product or when issues occur the market acts as a mediator between the buyer and seller, holding the money in escrow until an agreement has been reached. Buyers and sellers pay a small percentage of the transaction as escrow commission to the marketplace, which is usually around 2.5% [16].

Many markets use a 2-out-of-3 multisignature on top of the escrow service they provide. In these cases, the money is held in escrow in a so-called multisig wallet. Where traditional cryptocurrency wallets have one private key that is needed to authorise transactions, a multisig wallet has multiple. In the 2-out-of-3 multisig scheme used on most markets, multisig wallets are created with 3 signatures: one for the buyer, one for the seller and one for the market. Two out of three signatures are required to authorise any transaction. In this case the buyer and seller can agree that the goods have been delivered and authorize the transaction from escrow to the seller without interference of the market. At the same time, the marketplace can sign a transaction together with either the seller or the buyer in the case of a dispute. Another major advantage of this is that this prevents the market from using an exit scam and taking all the money in escrow, as more than one signature is needed to move the money in the account [17].

2.3.3 History of Darknet Markets

There are a number of large darknet markets that have been relevant in the last 20 years, the following Section elaborates on a timeline of the most well known and influential darknet marketplaces of the last 20 year. Though trade on the darknet was already present beforehand, the first real modern darknet market was established in 2011: Silk Road [18]. Silk Road was the first marketplace that used both Bitcoin escrow as well as Tor and was founded by ”Dread Pirate Roberts”, which was the pseudonym of Ross Ulbricht [19]. Silk Road remained the single largest darknet market until its takedown in October of 2013, as is explained in Section 2.3.4.

After the law enforcement action on Silk Road, more and more marketplaces started popping up on the darknet such as Silk Road 2.0, Evolution and Agora. Both Evolution and Agora even surpassed the original Silk Road in size [3]. At the same time Dream Market was also established.

In September 2014, AlphaBay was first launched. Roughly a year after the takedown

of the first Silk Road, in November 2014, an international law enforcement operation called Operation Onymous led to the seizure of over 25 Tor sites [20]. Among these sites was also Silk Road 2.0 as well as some smaller markets. The Agora market was not taken down during the operation, and surpassed the original Silk Road in size around the same time.

In March 2015, the two administrators of Evolution performed an exit-scam and stole around 12 million dollars worth of Bitcoin that was currently being held in escrow on the market [21]. Evolution only used a standard escrow system, and not a 2-out-of-3 multisignature scheme, allowing them to withdraw the money without issue [22]. In August of 2015, the Agora market announced its closure due to security reasons and asked all members to withdraw their money from the market [23]. At the same time that Agora market closed, Hansa Market was launched in August 2015.

By October 2015, AlphaBay had grown massively and was now recognised as the largest darknet market [24]. This stayed this way until Operation Bayonet in July of 2017, where both AlphaBay and Hansa Market were seized by law enforcement. In the case of Hansa Market, the marketplace was even briefly operated by law enforcement. Operation Bayonet is explained in more detail in Section 2.3.4. This seizure led to a change in the darknet market climate as users became more mistrusting and the environment slowly started to change from centralised marketplaces to decentralised marketplaces and direct chat services such as Telegram [25].

In 2019, Dream Market was the largest market by a long shot, with the second largest market being Wall Street Market. Dream Market shut down on April 30th 2019, whilst the owners of Wall Street Market have appeared to try to execute an exit scam around the same time [26]. However, this turned out not to be the case and instead the market was seized as part of a joint operation between European and U.S. law enforcement [27].

2.3.4 Previous Takedowns

In recent years law enforcement agencies all over the world have focused on taking down criminal marketplaces on the darknet. After taking down such a marketplace, agencies post a takedown notice such as the one in Figure 2.3, posted after the takedown of Silk Road. The main aim of these takedown notices is to deter users of the market to move to other markets. It also shows users that they are not untouchable on the darknet and can still be found by law enforcement.

Figure 2.3: Silk Road Takedown Notice [28]

Silk Road

The first time any worldwide attention was paid to darknet marketplaces was after the takedown of Silk Road by the Federal Bureau of Investigation (FBI). The advertised goods on Silk Road were mainly controlled substances and narcotics such as cocaine, amphetamines and cannabis [19]. Silk Road allowed a person to buy drugs anonymously using cryptocurrencies such as Bitcoin from anywhere in the world, as long as they used TOR and knew the specific .onion URL of the marketplace.

According to the FBI, they were able to determine the location of the servers hosting Silk Road due to a CAPTCHA service on the login page using content from the surface web. The connection with the surface web allowed the investigators to find the true address of the servers. However, experts have determined that there is limited proof for this claim by the government and speculate that other methods were used to find the servers [29].

On the 2nd of October 2013, the alleged mastermind behind Silk Road, Ross Ulbricht, was arrested in San Francisco. In the prosecution report published, it shows that for approximately 9.5 million Bitcoin in goods and services were traded on Silk Road [30], which at the time was worth around 1.2 billion dollars. In February 2015, Ulbricht was convicted of seven charges, including narcotics trafficking and computer hacking. On the 29th of May 2015, Ulbricht was given five sentences, out of which two were life imprisonment without the possibility of parole [31].

After the takedown of Silk Road, a new Silk Road (Silk Road 2.0) was relaunched in November 2013. The new market was led by administrators from the old Silk Road, who were quickly arrested in December 2013 [32]. Silk Down 2.0 ended up being taken down as a part of Operation Onymous in November 2014 [33].

AlphaBay & Hansa Market

In July 2017, a joint effort between the Dutch National Police and the FBI coordinated the shutdown of two large darknet markets within 16 days of each other. On the 4th of July, the FBI took down the darknet market AlphaBay, which at that time was the largest market online. Sixteen days later, the Dutch National Police took down Hansa Market, which was the second largest market (after AlphaBay) with the notice that they had actually been running the market for some time [34].

After AlphaBay suddenly disappeared without any explanation from its admins many users of the marketplace feared an exit-scam [35]. As later announced this was not the case, the marketplace was actually taken down by the FBI who kept quiet as per agreement with other law enforcement agencies. The reasoning behind hiding the takedown was that the second biggest marketplace at that time, Hansa Market, was being run by the Dutch National Police as a part of their operation [36]. Hansa Market was suspected to be the market where a lot of users would migrate to after the takedown of AlphaBay. This was confirmed by the fact that Hansa got an increase of 5000 users the day after the AlphaBay closure. The Dutch had found the Hansa server in Lithuania and created an exact replica in order to run the marketplace from the Netherlands. Whilst the actual servers of Hansa were taken down, the marketplace continued to operate through the Dutch server, allowing the Dutch National Police to act as admins of the marketplace. Users of Hansa had no idea that the marketplace was being run by investigators and thereby gave up a lot of their personal information without knowing. After 16 days the Dutch authorities took down Hansa Market and publicly announced that they had been running the market for over two weeks. Next to this they also published what information had been gathered during this time: a large number of unencrypted passwords and IP addresses as well as more than 10.000 physical mailing addresses [34]. After this, the FBI publicly declared that they had taken down AlphaBay and that the two takedowns were executed in collaboration as to gather as much intelligence as possible on the buyers and sellers on these marketplaces [37].

Data gathered from the running of Hansa Market was used in a number of ways. Next to arresting a large number of the top vendors of Hansa Market, the Dutch Police also performed in-person visits to the homes of users who bought goods on Hansa: ”knock-and-talk”-actions [38]. The users were informed of the fact that they have been identified by their purchases of illegal goods on the darknet and were either arrested or given a stern talking to depending on the amount of drugs bought [39].

2.4 Telegram

Telegram is an online messaging app along the likes of WhatsApp and Facebook Messenger that can be used to send messages via Wi-Fi or mobile data. Telegram has over 500 million monthly active users and is one of the 10 most downloaded apps in the world [40]. Telegram is developed with the specific intention to support

user privacy, which has many positive use cases. However, just like in the case of the darknet, this focus on privacy also means that it can be abused for illegal activities.

2.4.1 History

Telegram was founded in 2013 by two Russian brothers: Pavel and Nikolai Durov with the aim of providing a surveillance-proof messaging service to non-tech-savvy users. Before working on Telegram, the pair founded the Russian social network Vkontackte (VK), but were forced out by the Kremlin [41]. This due to the VK platform being used in the organization of mass protests against the results of the 2011 elections in Russia, which many people believe are were to be rigged in favor of the party of Vladimir Putin. After these protests, the Russian security service (FSB) asked VK to remove certain content related to the protests and to hand over specific user information, which Pavel Durov refused to do. This ultimately led to him having to sell his interest in VK and being exiled from Russia together with his brother [42]. In an interview Pavel Durov stated ”The no. 1 reason for me to support and help launch Telegram was to build a means of communication that can’t be accessed by the Russian security agencies” [43].

After their exile from Russia, the brothers split the work on Telegram with Nikolai creating the protocol on which the messenger would be based on: MTProto, and Pavel providing financial support. The iOS version of the app launched on the 14th of August 2013 and the Android app officially launched on the 20th of October 2013. Due to the popularity of Pavel Durov, the app immediately gained a lot of users in Russia. A few months after the launch of Telegram, Facebook announced their takeover of one of the main competitors of Telegram: WhatsApp. Due to Facebook’s plans regarding data monetization and advertisement many users disregarded WhatsApp and started looking at different messaging applications, resulting in over 8 million Telegram downloads in just a few days [43]. Telegram is registered as a British LLP and uses a series of shell companies registered all over the world. The main reason for this structure is to help the company evade requests from governments for user information as well as content restrictions [44].

2.4.2 Telegram Functionality

According to Telegram's own FAQ, Telegram is a cloud-based messenger that uses seamless sync to allow users to view their messages across their app on any platform. Telegram can be used on almost all smartphones, tablets and computers. There are apps for iOS and Android as well as desktop apps for Windows, MacOS and Linux. Next to this there is also a native MacOS app and an online Telegram Web app that users can use to access their Telegram via any internet browser [40]. There are a number of different ways in which users can communicate on Telegram:

- **User-to-user:** Specific chats for two users where they can send messages to each other without any other users viewing and participating in the chat.
- **Groups:** A group can have up to 200.000 members. All members in a group can send messages to the group, and receive messages sent to the group. Groups are managed by group administrators. There are two different ways in which a group can operate, all members can be in control of the name and photo of the group, as well as being able to invite new members to the group. The second way of operation is a restricted group, in which a only administrators are allowed to change the name and photo, as well as add and remove people from the group. There is also the option of persistent memory, so new users who are added to the group are also able to see the history of the group [45].
- **Channels:** Channels differ from groups in that not all users can send messages. Only the administrators of a channel can broadcast messages in it, with most channels being managed by one or just a few administrators. Channels can be followed by an unlimited number of users, which is different to the 200.000 user limit on groups. When a message is posted in a channel, it gets signed by the channel name and photo instead of the name and photo of the user sending the message. Every message in a channel also has a view counter that is updates when a message, or its forwarded copies are viewed [40], [46].

Users of Telegram can either contact people who are in their phone contact list and are also using Telegram, or contact people via their Telegram username. Telegram also has a 'People Nearby' option that allows users to find other Telegram users in the area to chat with [40]. As a privacy protection measure only an approximate location of a user is used in the People Nearby function.

2.4.3 Secret Chats

Next to normal user-to-user chats already elaborated on in Section 2.4.2 Telegram provides users the option to create a Secret Chat. Secret Chat uses end-to-end encryption, only allowing the sender and receiver to decrypt and read the messages. Next to this, secret chat also does not allow the forwarding of messages. If a messages is deleted by one of the two users, then the app of the other user will be ordered to delete that specific message as well.

Secret chat messages are only able to be accessed on their devices of origin, so if a user were to switch devices the chat will not be transferred [41]. It is also possible to send self-destructing messages. These are messages which have a timer which starts counting down as soon as the message is displayed on the receiver's screen. As soon as the timer runs out, the message will self-destruct and be deleted from both devices [40].

2.4.4 Privacy & Security

Telegram promotes itself as a messaging app with a big focus on security. Since the start Telegram has been a messaging app that is 100% free and does not show ads or sell user data. However, due to Telegram now having almost half a billion active users, changes needed to be made in order for the company to keep afloat among the rising traffic and server costs. Therefore, starting in 2021 Telegram introduced monetization in certain aspects of their app to generate revenue. This entailed that some business features would become paid features and that Telegram would introduce their own Ad Platform for public one-to-many channels to allow channels to display ads to earn money [47].

Telegram is based on the MTProto protocol, which is developed by the Telegram team themselves. The reason for using a custom protocol instead of an already existing protocol is because of reliability on relatively weak mobile connections. Two types of encryption are used in messages on Telegram: private chats and group chats use server-client encryption whilst the secret chats use end-to-end encryption. All data is encrypted in the same way and the encryption is based on 256-bit symmetric AES encryption, 2048-bit RSA encryption and Diffie-Hellman secure key exchange [40]. Messages sent in secret chats are not stored on Telegram's servers and can only be accessed on the devices of origin.

Telegram provides users the possibility to contact their GDPRBot in order to request a copy of all their data that Telegram stores as well as contact them about Data Privacy and their privacy policy [40]. The creators of Telegram have run contests in the past where users were challenged to crack the encryption of the messaging app with prizes up to $300,000 [48]. Next to this, Telegram also has an active bug-bounty programme to reward the finding of security flaws and bugs in the messaging app and protocol.

2.4.5 Telegram API

Telegram API and code is open-source. However, the code does contain binary blobs. These blobs are executable binaries that the code uses that do not have publicly available code and can therefore not be analyzed. [41]

Chapter 3

Related Work

In the following Section previous literature on criminal marketplaces on both the darknet as well as Telegram will be discussed.

Research done by Georgoulias et al. [49] investigates the operation of 41 marketplaces and 35 vendor shops on the dark web. All the marketplaces and vendor-shops were operational at the time of the paper, where specific data needed for the research was scraped from the marketplaces. All marketplaces and vendor shops were compared in terms of Access & Authentication, Products & Purchases, Shipping & Delivery, Vendor Reputation, Support, Disputes & Community and Marketplace Revenue to find out what makes a dark web marketplace successful. The authors concluded that trust is one of the most vital pillars on which dark web marketplaces are run, as trust plays a vital role in the inner workings of the market.

Nunes et al. [50] presented a system for intelligence gathering on sites on the darknet and deepnet. The system specifically focused on the collection of information from hacker forums and criminal marketplaces offering hacking services. Their research also elaborates on two case studies one of which where the system is used to discover zero-day exploits in marketplace data.

In research written by Christin [51] an extensive measurement analysis of the Silk Road darknet marketplace is done. Daily crawls of Silk Road were executed for a period of six months, with the primary focus on product item pages describing goods for sale. Main conclusions were that drugs were the most popular items on Silk Road, that there is an international community behind the marketplace and that users stay active on the site for a relatively short period of time.

Pastrana et al. [52] created a designated crawler for criminal underground forums:

CrimeBot. This crawler is designed to be stealthy and gather as much information as possible and all data is stored in a database called CrimeBB. The CrimeBB dataset is available for academic researchers to use.

Benjamin et al. [53] have created a framework for conducting darknet identification, collection and evaluation with ethics, the DICE-E framework. This framework provides a complete guideline for scholars on Darknet research. They compare a number of previous studies in terms of their data sources, data collection, analytical methods and findings to gather information on how to best research forums and marketplaces on the darknet. DICE-E elaborates on four research phases: darknet identification, data collection, evaluation and ethics.

Research done by Décary-Hétu et al. [54] investigate law enforcement's actions against criminal underground marketplaces. The authors argue that disruption methodologies would serve a better result than the current investigate-then-arrest methodology used by most law enforcement agencies. For this a dataset was used containing all activity (posts, profiles and private messages) from the GhostMarket online forum.

Lacson et al. [55] analyze the aftermath of the fall of the darknet market Silk Road to draw conclusions about the behavior of the users of darknet markets. A forum set up just after the fall of Silk Road to discuss the theorie on how the market was taken down was scraped and evaluated as well as two competing markets of Silk Road: Agora and Evolution. The main finding in terms of users avoiding the darknet or switching to a different market was that even though the largest darknet market was taken down, darknet marketplaces overall have expanded considerably since.

Research done by Amarasingam et al. [56] focuses on the use of Telegram groups and channels as a jihadist platform. The research covers a dataset containing 7.8 million Telegram posts gathered from 1,911 different channels, groups and supergroups associated with jihadist extremism from 2015 to 2019. Data was crawled from the different channels and groups using Telegram's API. The data was used to understand the impact of two Europol Action Days in 2018 and 2019 on the number of unique posts and the movement of users between different groups, as well as the longevity of channels and groups. An interesting point of this research is that it focuses on the aftermath of specific takedown actions by looking at both the user movement as well as the increase or decrease in the use of other communication groups.

That Telegram is used more and more in criminal and terrorist circuits is also endorsed by research done by Weimann [57]. They evaluate the migration of terrorists

to both the dark web and messaging applications in terms of their internal communication as well as communication to the outside world. After the launch of the channels feature on Telegram in September of 2015, the Terrorism Research & Analysis Consortium (TRAC) witnessed a massive migration from other social media sites to Telegram.

Peter et al. [58] present an efficient way of creating a dataset from relevant Telegram channels and groups which can be used to detect clusters in the network and find influential actors. In their research they focus on Telegram channels and groups from German COVID-19 sceptics and aim to find the most influential channels, actors and communities within the data. They also investigate the growth and evolution of the network compared to the pandemic measures from the German government. Communities are identifies using the Louvain method whilst the most influential channels and groups are determined using PageRank. This paper also mentiones TeleGram-Scraper [59] and Telescrape [60] as similar tools for the investigation of Telegram groups and channels to the one developed during the research.

In recent research of Blankers et al. [61], the evaluation of online psychoactive substance trade during the COVID-19 pandemic via Telegram is investigated. Data was gathered by subscribing to 3 large Dutch Telegram market groups found using the ”drugs” search term in the Telegram search engines. Messages were downloaded using the Telegram desktop client software. Conclusions made were that social media such as Telegram are most likely used for the purchase of smaller amounts of drugs, which is different compared to darknet markets.

Moyle et al. [62] investigate how smartphone-enabled social media and messaging applications are used for the buying and selling of drugs. Using a range of methods to interview drug users, over 400 interviews were held to gather information. One of the key takeaways from the research is that the convenience of buying drugs using various social media apps, such as Telegram, is far higher than when using the darknet. The disadvantages of using marketplaces on the darknet to obtain drugs was highlighted due to the need for more technical expertise and the easy operability of messaging apps.

Wang et al. [63] also investigated the criminal marketplaces hosted on Telegram channels and groups. In their observation, criminals often use jargon in their messages instead of sensitive terms to avoid detection. Therefore, a jargon identification framework (Chinese Jargons Identification Framework) was created to automatically identify jargons in the messages. To gather the data, 12 Telegram groups active in transactions in underground markets such as selling drugs and guns were crawled

for a period of 2 months.

Chapter 4

Dataset

The following chapter describes the two datasets that will be used during this research. The data in both datasets has been gathered by the Dutch National Police as part of investigations into the actors behind the different marketplace platforms.

4.1 Darknet Marketplaces

For this study we will be using the datasets of three Darknet marketplaces that operated in the last ten years: Wallstreet Market, Hansa Market and Alphabay. At some point in time each of these three marketplaces were the biggest criminal marketplace on the darknet. Information on the total number of users and the measurement period for the three marketplaces can be found in Table 4.1.

For all three marketplaces data is present from the initial setup of the marketplace up until the shut down. For the first few weeks of which there is data for the three marketplaces they were still closed to new users, as the marketplaces were being set up. Therefore we will only use the data from the datasets starting from the point in time where the marketplaces were publically accessible. This results in 924 days

Marketplace	Number of users	Start data collection	End data collection
Wallstreet Market	1,150,842	16-10-2016	24-04-2019
Hansa Market	420,274	18-03-2015	20-07-2017
Alphabay Market	1,859,973	27-07-2014	19-07-2017

Table 4.1: Dataset information Darknet marketplaces

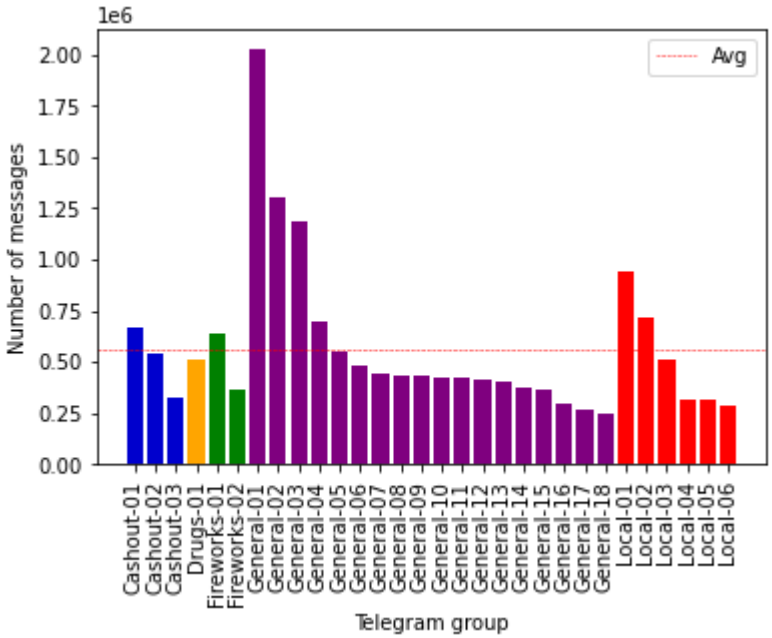


Figure 4.1: Number of messages sent in each Telegram Group

of data for Wallstreet Market, 861 days of data for Hansa Market and 931 days of data for Alphabay.

4.2 Telegram Groups

We will also use a Telegram Dataset which contains a large database of messages sent in a number of different Telegram groups. For this dataset we have access to a rolling window of data going back a year. Therefore we will only be looking at entries during our defined measurement period. We have defined this measurement period as 01-02-2022 up to and including 01-12-2022, giving us 10 months of data. The entire dataset contains messages from 301 different Telegram groups. However, a large portion of these groups only contain a limited number of messages. To find the most used and most active Telegram groups to use in our study we look at the number of messages sent over the duration of the measurement period. As there is a large number of Telegram groups in the dataset, we specifically focus on the groups where the most messages are being sent. Therefore we take the top 10% of the 301 groups: the 30 groups in which the most messages are being sent. Each of these 30 groups will be given a pseudonym according to the predominant category of messages sent in the group. We divide the groups into the following five categories:

- Cashout-focused groups contain messages and advertisements focused on fraud, money laundering, stolen credit and debit cards.
- Drugs-focused group contain messages and advertisement focused on soft and hard drugs such as cannabis, weed, cocaine and heroin.
- Fireworks-focused groups contain messages and advertisements focused on (illegal) fireworks.
- Local-focused groups contain messages and advertisements not specifically focused on one category of services and goods, but are focused on one specific area of the Netherlands.
- General-focused groups are the groups that do not fit into any of the above mentioned categories.

Using these categories the 30 groups contain 3 Cashout-focused groups, 1 Drugs-focused group, 2 Fireworks-focused groups, 6 Local-focused groups and 18 General-focused groups. Figure 4.1 shows an overview of the number of messages sent in each of the top 30 Telegram groups. Group General-01 is the biggest group in terms of messages, containing over 2 million messages. The smallest group in the dataset is General-18, containing a little under 250.000 messages.

Chapter 5

Methodology

The following chapter contains the methodology used to generate our results. Section 5.1 describes the approach used to get information on the administrators, moderation methods and payment methods of the marketplaces. In Section 5.2 we explain the ways in which we compare the users for the different marketplaces. Next, Section 5.3 explains the approach used to compare the goods and services on both marketplaces, including the ground truth and classifier used to analyse the messages in the Telegram groups. Finally, Section 5.4 elaborates on the methods used to compare the development of the marketplaces over time.

5.1 Organisational Structure

We first start comparing the two types of marketplaces by looking at their organisational structure, as defined by research question SQ1 in Section 1.2 . All marketplaces have people and systems behind them that are vital to the operation of the marketplace.

5.1.1 Administrators

The Darknet marketplace dataset contains separate entries for each of the user accounts in the marketplaces. Each of these user entries has a 'User Type' variable which can have a number of different values. This User Type can be used to distinguish between normal users, admins, banned users and deleted accounts. As we want to know how many administrators the marketplace has, we specifically look at

the users where the User Type is ‘Admin/Founder’.

Next to the User Types, the marketplaces also have different ‘User Groups’. These groups contain users with specific rights or functions within the marketplace. Each of the marketplaces have ‘Buyer’ and ‘Vendor’ User Groups. However, Alphabay also has an ‘Administrator’, ‘Moderator’, ‘Manager’ and ‘Public Relations’ groups which we will also take into account when calculating the number of Administrators.

Users in Telegram groups can be divided between normal members and admins. Admins can be appointed by the group creator/owner and other administrators to help manage the group. Owners can set up administrator rights for each individual administrator when they are appointed. This means that different administrators can have different administrator rights. For example, one administrator might be able to ban users, whilst another cannot. Originally, administrators could be identified by the tag ’admin’ next to their name and messages.

In the Telegram update of August 9th, 2019, Telegram added the feature of custom admin titles. This allows administrators to change their title in the group from the regular ‘admin’ to anything they want [64]. The September 2020 Telegram update [65] also makes it possible for admins to remain anonymous by using the anonymous admin feature.

The combination of these two features makes it difficult to find the owners and all administrators of a group, because a portion or all of the admins (including the owner) might be hidden from view. Next to this, there are also a number of group moderator bots that can take over a large portion of the admin work. Therefore, we look at all visible users in the user lists for all the Telegram groups that have a title. As only administrators and owners can change their titles, this allows us to establish a lower bound to the number of administrators of each of the Telegram groups.

5.1.2 Market Moderation

There are a few different ways in which the Darknet marketplaces and Telegram groups are moderated. In the case of the Darknet marketplaces users have the possibility to open a dispute on a sale if they are not satisfied. Next to this, users also have the possibility to give feedback on the vendors after an order has been finalised. Disputed and direct feedback for orders on the Telegram groups are usually handled through private messages between the buyer and vendor, with the exception of some general feedback messages being sent in the Telegram groups. However, the

Telegram Groups often do use bots to manage and moderate the messages sent in the groups.

Darknet Marketplaces - Disputes

Wallstreet Market offers both sellers and buyers the possibility to open a dispute when an order does not go as expected and seller and buyer cannot come to an agreement themselves. The payment is still held in escrow by the marketplace, as the seller and buyer have not come to an agreement yet and therefore the market is able to mediate and decide on a verdict. The market can rule in favour of the buyer and refund the buyer, or it can rule in favour of the seller and have the payment go through. When a user opens a dispute on a transaction, they are asked the reason for the dispute and are given the option to provide further comments. After these details have been provided, both the seller and the buyer receive a message from the marketplace stating: 'A dispute was initiated. The administration will review this case within the next hours. The transaction is muted during this time.' A moderator is assigned to the dispute and will decide on the ruling of the dispute based on the details provided by both the buyer and seller. All disputes are given a status: a resolved status if the dispute has been closed or handled, or an unresolved status if the dispute has not yet been handled. Disputes containing a dispute status of "Status: Resolved" are counted as resolved disputes, whilst disputes containing a dispute status of "Status: Unresolved" are counted as unresolved disputes. Disputes that are resolved also have a note attached stating if the dispute was resolved in favour of the seller or the buyer.

Hansa Market uses the same dispute system as Wallstreet Market. Again we can find the number of unresolved disputes by looking at the dispute status "Status: Unresolved". Similarly, we get the number of resolved disputes by looking at the disputes containing a status of "Status: Resolved".

Alphabay uses a slightly different way of handling disputes. Instead of the dispute system they handle disputes through private message conversations between the assigned moderator, seller and buyer. Disputes are removed from orders after they have been closed, therefore the number of disputes in the dataset is the current number of unresolved disputes. However, a notification is generated each time a buyer or seller creates a dispute on an order, which we can use to determine the total number of disputes. As the disputes are handled through private messages and each moderator handles the dispute process in a different way it is unclear how many of the resolved disputes ended up in favour of the buyer or seller.

Darknet Marketplaces - Feedback

All three marketplaces make use of a feedback system to help potential buyers choose vendors to buy from. Buyers have the option to leave a numerical rating as well as a comment explaining their rating about the vendor after their order has been finalised. This is the case when the buyer has received the goods and the seller has received the funds after they have been released from escrow. The difference between the three feedback systems on the darknet markets is the numerical values they use for ratings:

- Wallstreet Market uses a rating scheme between 1 and 5. The lowest rating is a score of 1, whilst the highest rating is a score of 5.
- Hansa Market uses a negative (-1), neutral (0), positive (1) rating for all their orders.
- Alphabay uses a rating scheme between 1 and 3. The lowest rating is a score of 1, whilst the highest rating is a score of 3.

In order to compare the ratings for all marketplaces, we specify three overall ratings: positive, neutral and negative. In the case of Wallstreet Market, the 4- and 5-point ratings are classified as positive ratings, the 3-point ratings as neutral ratings and the 2- and 1-point ratings as negative ratings. Hansa Market's feedback ratings are already classified in terms of positive, neutral and negative and therefore we do not change anything. Alphabay's ratings are classified as 3-point ratings being positive, 2-point ratings being neutral and 1-point ratings being negative.

Telegram - Bots

To help the administrators run the Telegram groups, most groups make use of bots. Some bots only do as little as removing messages containing URLs. Other bots can be used to completely manage an entire group with banlists, banned words, specific member permissions and scheduled posts. Each of the messages in the Telegram dataset contains a SentByBot variable that is set to True when the message is sent by a bot instead of a normal user. We use this variable to determine the number of messages for each of the bots in the Telegram groups. Using this data we can count how many bots send messages in each of the groups as well as the percentage of messages sent by bots.

5.1.3 Payment Methods

Each item listing on the three Darknet Marketplaces has a price associated with it. This price is usually stated in euro, US dollars or bitcoin. Vendors can list the accepted payment methods for each of their listings. Therefore, in order to find the different payment methods and how widely they are accepted on the marketplaces we look at the payment methods for all listings. Multiple payment methods can be linked to a single item listing. For example, it is possible to pay for a listing with both Bitcoin and Ethereum. Therefore we visualise the usage of a payment method as a percentage of the total items for each of the payment methods separately.

To determine what payment methods are actually used to pay for the orders we look at the database containing all the orders. Each of the orders has a payment currency associated with it, so using this database field we can find out how many orders have been paid for using a certain payment method. To find out what payment methods are used and accepted for goods and services sold through the Telegram groups we look at the texts of the advertisements placed in the groups.

5.2 Users

To compare the users of the Darknet marketplaces and the Telegram groups, we look at a number of different properties. We will compare the total number of users, of which the approach is elaborated on in Section 5.2.1. Next, we will also look at the number of active users and the number of vendors as explained in Sections 5.2.2 and 5.2.3

5.2.1 Total Number of Users

To determine the total number of users on the Darknet marketplaces we look at the number of individual users accounts present in the dataset. Test accounts used by the creators of the marketplaces during the setup of the marketplace (before the marketplaces were accessible to others) may have registration dates that have been modified. For example, registration dates for these test accounts may be the Unix epoch. Therefore, only user accounts that have a valid registration date between the start of the marketplace until its closure are counted to determine the total number of users. This is done for all three marketplaces separately.

To determine the total number of users for each of the groups in the Telegram datasets we query the data present in the database for the duration of the measurement period and execute a cardinality count on the actor.username field. This count will count the number of unique values in the actor.username field. As usernames are unique for each user, this gives us the number of unique users for the Telegram group. In the case where the specific Telegram group categories are combined each of the groups is given an equal weight to determine the combined value.

5.2.2 Number of Active Users

The number of active users for both the Darknet marketplaces as well as the Telegram groups is calculated according to the method described in Section 5.4.1 which gives us a list of the number of active users for each week in the measurement period.

The average number of active users for each of the Darknet marketplaces and Telegram groups is then calculated by taking the average of all values in the list of the number of active users per week. The percentage of active users is calculated using the average number of active users which is divided by the total number of users, which is calculated as explained in Section 5.2.1.

For both the average number of active users and the percentage of active users, the data of the Telegram groups is also grouped by category. To determine the averages of each of the categories, each of the groups is given the same weight.

5.2.3 Vendors

In order to compare the number of vendors and their number of listings we need to find out who the vendors are on both the Darknet marketplaces and in the Telegram groups. In the case of the Darknet marketplaces, all vendors first have to apply to become a vendor and pay a vendor fee. After this vendor fee has been paid these users get the ability to publish listings and sell their goods and services. For all three of the Darknet marketplaces in our dataset, vendor users are part of a specific vendor user group. This makes it easy to get the number of vendors from each of the marketplaces. Using this number of vendors we also calculate the percentage of vendors compared to the total number of users as well as the average number of listings per vendor. To calculate the number of listings per vendor we use the total

number of listings on the marketplace and divide this by the number of vendors.

It is more difficult to get the vendors from the Telegram groups. In order to get the number of vendors we use the classifier explained in Section 5.3.2 to get the information on all advertisements in the Telegram groups. For each of the advertisements we save the unique user identifier of the sender and a hash of the message text. This way we get a list of all unique users that place advertisements in the Telegram group: the vendors. Using the hashes of the message texts we can also distinguish how many different advertisements are sent by each user. We calculate the percentage of vendors in terms of the total number of users in the groups, as explained in Section 5.2.1.

5.3 Goods & Services

To be able to compare the goods and services being advertised on the different marketplaces, all these advertisements need to be classified in a general pattern equal for all data. To carry out this research we need to give all messages in the Telegram dataset a meaningful classification. In order to do this we rely on a classifier that has been developed by myself and three others as part of a course of the Cybersecurity Master's programme at the University of Twente [66]. Therefore, all advertisements will be sorted into one of 11 different general categories, based on the categories used in the classifier explained in Section 5.3.2. The categories we consider are the following:

- Weapons (Tasers, Knives)
- Firearms and explosives (Guns, C4, Ammunition)
- Fireworks (Illegal Fireworks)
- Licenses and Personal Documents (Fake driving licenses, Personal Identification Documents, Certificates of Good Conduct, College Degrees)
- Stolen Goods (Stolen Cars, Clothes, Electronics, Scooters, Bikes)
- Soft Drugs (Soft Drugs as classified by the Dutch Opium Act [67], Cigarettes, Alcohol)
- Hard Drugs (Hard Drugs as classified by the Dutch Opium Act [67])

- Pharmaceuticals (Xanax, Antidepressants, Erection pills, Sleeping pills)
- Cashout (Fraud, Money Laundering, Stolen Credit Cards)
- Cybercrime (Phishing Panels, Hacking Automated Systems, Digital Scams, Digital Subscriptions)
- Other (Prostitution, Pornography, Match Fixing, other advertisements that do not fall under any of the other categories)

Advertisements in the three darknet marketplaces datasets are already categorised into more specific categories than the 11 categories stated above. Therefore these categories will be sorted into one of the 11 categories manually. For example: the category ”Weed” is classified as part of the ”Soft Drugs” category and the category ”Exploit Kits” is classified as part of the ”Cybercrime” category.

Data from the Telegram dataset is unsorted and therefore some processing needs to be done before the data from the two datasets can be combined. Therefore, we will be using two Machine Learning classifiers as explained in Section 5.3.2 trained by a ground truth of labeled Telegram messages to classify each of the messages in the Telegram datasets.

Firstly, a classifier will be used to determine if a message is an advertisement or a non-advertisement. Advertisement messages are messages where an item or service is promoted as available for purchase, or messages where a specific item or service is requested. An example of an, clearly fictitious but realistic, advertisement message offering an item or service is:

> *ThePotatoFarm:* New potatoes for sale! Get 20 kgs for only €15.00! DM for more information.

An advertisement message containing a request for an item or service can look like:

> *IWantPotatoes:* Does anyone have 20 kgs of Potatoes for sale? DM me if you can help me.

Non-advertisement messages are either chat messages, or bot-notification messages. Chat messages are messages where no goods or services are being offered or requested. For example, a chat message can look like:

PotatoesAreStupid: I hate potatoes!

Bot messages are automatic messages sent by bots in the group. These bots can do a number of different things, mostly explaining and enforcing rules. A bot message can look like this:

PotatoBot: User 'PotatoesAreStupid' has been banned.

Secondly, a classifier will be used to determine the advertisement category of a message based on the previously described list of categories. This classifier will only be executed on the messages that have been classified as an advertisement by the first classifier, as classifying non-advertisements has no use. The Telegram Message classifiers have been developed by 3 other researchers and the author of this paper as part of an unpublished deliverable for the course Cyber Crime Science and have been adapted to work with the current dataset.

5.3.1 Ground Truth

The ground truth is a dataset containing 18.836 manually labeled Telegram messages of 47 different Dutch Telegram groups. In each of the 47 groups a random sample of between 225 and 900 messages was labeled and became part of the ground truth. This to make sure that the ground truth is not skewed by a larger number of messages from a single group. In total the ground truth contains 13.483 advertisement messages (71,58%) and 5.353 non-advertisement messages (28,42%).

Table 5.1 shows the percentage of messages in each of the categories compared to the total number of messages in the ground truth. These percentages sum up to 105% instead of 100%. This is because there are messages in the ground truth that advertise items in multiple categories in the same message. For example, a singular message can advertise both Soft Drugs and Hard Drugs and therefore needs to be classified as both belonging to both categories.

	Percentage
Weapons	0,64%
Firearms and Explosives	1,54%
Fireworks	3,51%
Licences and Personal Documents	3,80%
Stolen Goods	5,10%
Soft Drugs	15,41%
Hard Drugs	11,90%
Pharmaceuticals	2,62%
Cashout	35,38%
Cybercrime	18,62%
Others	6,79%

Table 5.1: Ground Truth Category Percentages

5.3.2 Classifier Pipeline

Both classifiers are trained using the ground truth described in Section 5.3.1. However, before using the classifier, the data is first cleaned, tokenized and transformed[1]. The data is cleaned by converting all letters to lowercase letters and removing any numbers and symbols. Next, tokenization is performed. Tokenization is a method of splitting textual input data into individual tokens that can be further processed by machines. We tokenize all unique words and bigrams (a two-word sequence of words, such as ”this is” and ”is different”) in the cleaned dataset. For each token we calculate the term frequency times inverse document frequency (tf-idf), which is a statistic that reflects how important a word is to the text. We use this as a weighing factor to scale down tokens that appear more frequently than others. For example the word ’advertisement’ has a higher importance in a text than the word ’the’, however ’the’ appears a lot more and therefore has a higher tf-idf value. Finally, we use a Stochastic Gradient Descent model to find the optimal parameter configuration for our machine learning algorithm.

The first model is trained to classify the message category in terms of advertisement or non-advertisement. A train-test split of 80% training data and 20% testing data was used to evaluate the performance othe model. The model classifying the mes-

[1]Classifier created based on setup from `https://scikit-learn.org/stable/tutorial/text_analytics/working_with_text_data.html`. For more information on the classifier contact the author.

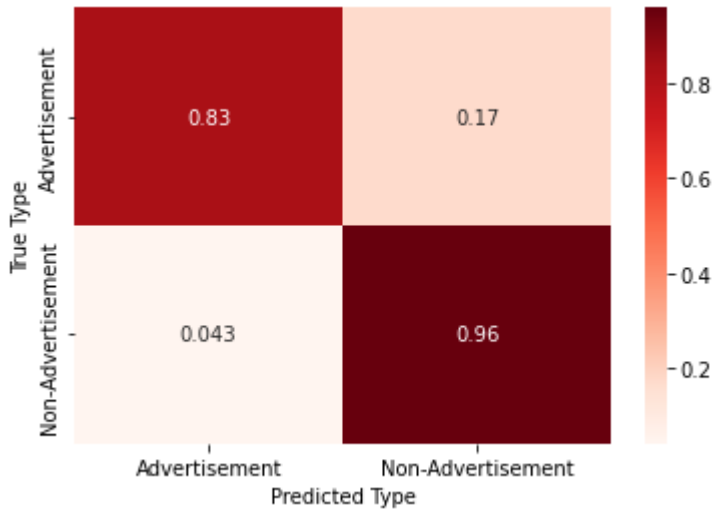


Figure 5.1: Confusion Matrix Advertisement classifier model

sage category has an average accuracy score of 91% , an average precision score of 93% and an average recall of 94%. The confusion matrix for this model can be found in Figure 5.1.

The second model is trained to classify the advertisement category in terms of one of the eleven advertisement categories. Again, a train-test split of 80% training data and 20 % testing data was used to evaluate the performance. Resulting in an average accuracy score of 84%, an average precision score of 85% and an average recall score of 75%. Figure 5.2 shows the confusion matrix of this model. Both models are written in Python code using Jupyter Notebooks and the sklearn and pickle packages.

5.3.3 Implementation

Categories of advertisements in each of the three Darknet marketplaces are manually sorted into one of the eleven categories stated at the beginning of this section. The corresponding results are visualised in tables and graphs using the pandas and matplotlib Python 3 packages.

The classifying of the Telegram group messages is a bit more complicated. Firstly, the previously described classifier models are trained using the ground truth described in Section 5.3.1. Next, a specialised ElasticSearch query is used to query a maximum of 10.000 entries from a single Telegram group at a time. The specific message text is then gathered from each entry, after which the first classifier model predicts the message type for each of the message texts. All message texts that

Figure 5.2: Confusion Matrix Categories classifier model

are classified as advertisements are then processed by the second classifier model, which predicts what category the advertisement message belongs to. Count values for the advertisements and categories are saved and the next group of 10.000 entries is queried. The ElasticSearch query uses a sliding window to ensure that every message in a Telegram group is queried exactly once. If no more unqueried entries exist for the current Telegram group, the results for the current group are saved to a file and the program continues querying the next group. This continues until all messages in all groups for the specified time period have been queried and classified. This program is written in Python 3 Jupyter Notebooks, using the pandas, pickle, sklearn, elasticsearch and numpy packages.

The previously generated result files for each of the Telegram groups are used to generate visualisations using the matplotlib and seaborn Python packages. When multiple groups are combined, such as per Telegram group focus, each of the groups is given an equal weight as not to skew the results. Similarly, when the three darknet marketplaces are combined each of the marketplaces is given an equal weight. All this data is used to analyse the contents of both datasets and the individual groups and marketplaces. Section 8 shows the results for both the Darknet marketplaces as well as the Telegram groups after classification.

5.4 Development over Time

In order to compare the usage of both Darknet marketplaces and Telegram groups over time, we will look at both the users and messages over time. The total number of active users will be compared for both datasets, as well as the relative growth and the number of new and leaving users.

While the Darknet marketplaces might contain a large number of user accounts, this does not mean that all of these accounts are actively being used. Therefore using the total number of users can give a skewed view of the size and activity on the marketplace. Each user account has a 'First Seen Time' and 'Last Seen Time' value containing the date and time at which the user account first and last logged in on the marketplace. We therefore define a user to be 'active' between the dates of the First Seen Time and Last Seen Time, including both first and last seen dates.

> *For example: User "PotatoFarmer" registered on the marketplace on 01-03-2017 at 17:05 and therefore has a First Seen Time value of 01-03-2017 at 17:05. Their Last Seen Time value is 01-05-2017 at 13:34.*

Therefore, we classify the user "PotatoFarmer" as being an active user between 01-03-2017 and 01-05-2017 inclusive.

We define users in the Telegram groups as active in a similar way. In the Telegram groups we take the date of the first and last message users have sent in a group and define these users being active in the period between those dates inclusive.

For example: User "ILovePotatoes" sent his first message in Telegram group "EverythingAboutPotatoes" on 03-02-2022 and their last message on 15-06-2022. Therefore, we classify "ILovePotatoes" as being an active user of group "EverythingAboutPotatoes" from 03-02-2022 up to and including 15-06-2022.

In this case it is important to note that the data for the Telegram groups does not contain all data that has ever been sent in these groups, but only the ones sent within the measurement period. Therefore, there might be messages in the group before the measurement period starts and users might have already been active in the groups for longer. Similarly, the groups continue to operate after the measurement period has ended, giving the possibility that users might still send messages after this end date. Therefore, this can give skewed data in the first and last weeks of the measurement data. As a lot of users might appear as 'new users' for the first time during the measurement period in the first few weeks, but have already been members for longer. The same applies for 'leaving users' as they might appear to be leaving as their last message is sent in the last weeks before the end of the measurement period. Therefore we disregard the data from the first and last month, to get an accurate overview of the normal workings of the groups.

5.4.1 Number of Active Users

For both the Darknet marketplaces and the Telegram groups we calculate the number of active users per week. To calculate this we use the number of new users and leaving users. In the case of the Darknet marketplaces we define a user as being new in the week of their First Seen Time and as leaving in the week of their Last Seen Time:

For example: User "PotatoFarmer" registered on the marketplace on 01-03-2017 at 17:05 and therefore has a First Seen Time value of 01-03-2017 at 17:05. Their Last Seen Time value is 01-05-2017 at 13:34.

Therefore, we define this user as being a new user in the week of 01-03-2017, which is in the week of 27-82-2017 to 03-03-2017. This user is defined as a leaving user in the week of 01-05-2017, which is the week of 01-05-2017 to 07-05-2017.

Similarly, we define a user in a Telegram group as being new in the week of their first message in the group, and as being leaving in the week of their last message in the group:

For example: User "ILovePotatoes" sent his first message in Telegram group "EverythingAboutPotatoes" on 03-02-2022 and their last message on 15-06-2022. Therefore, we define this user as being a new user in the week of 03-02-2022, which is in the week of 31-01-2022 to 06-02-2022. Equivalently, we define this user as being a leaving user in the week of 15-06-2022, which is the week of 13-06-2022 to 19-06-2022.

We then calculate the number of active users for week k, denoted as $U_{active}(k)$, as follows:

$$U_{active}(k) = U_{active}(k-1) + U_{new}(k) - U_{leaving}(k) \tag{5.1}$$

$$U_{active}(0) = 0$$

Where $U_{new}(k)$ is the number of new users in week k and $U_{leaving}(k)$ is the number of leaving users in week k. Due to the reasons with skewed data stated above, the first and last 3 weeks of the data for the Telegram groups are not visualised.

5.4.2 Relative Growth

We want to compare the growth of the Darknet marketplaces to the growth of the Telegram groups. As the sizes of the different marketplaces and groups differ by hundreds of users we use the relative growth for each week to be able to accurately compare them.

To calculate the relative growth of a group or marketplace in a week we use the total number of active users for that week and the week before. Therefore, we calculate the relative growth in week k, denoted as $R_{growth}(k)$, as follows:

$$R_{growth}(k) = \frac{U_{active}(k) - U_{active}(k-1)}{U_{active}(k-1)} * 100 \tag{5.2}$$

Where the $U_{active}(k)$ is the number of active users in week k as calculated by Equation 5.1.

The first and last three weeks of the data for the Telegram groups are not show in the graphs, due to reasons stated above. Because we want to compare both types of marketplaces when they are up and running marketplaces, we have decided to omit the first and last three months of the Darknet marketplaces from the visualisation.

5.4.3 New and Leaving Users

The relative growth percentage only says something about the percentage of new and leaving users combined, not about each of them individually. As a relative growth of 10% could mean an increase of 60% for new members and a decrease of 50% for leaving members. However, a relative growth of 10% could also mean a 12% increase in new members and 2% of the members leaving. Therefore it is important to also look at the percentages for new and leaving users separately.

We denote the percentage of new users in week k as $P_{new}(k)$ and calculate it as follows:

$$P_{new}(k) = \frac{U_{new}(k)}{U_{active}(k-1)} * 100 \tag{5.3}$$

Where the $U_{active}(k)$ is the number of active users in week k as calculated by Equation 5.1 and $U_{new}(k)$ is the number of new users in week k. We use the total number of active users in the previous week $U_{active}(k-1)$ to get the increase percentage of new users in the current week.

Likewise, we denote the percentage of leaving uses in week k as $P_{leaving}(k)$ and calculate it in the following way:

$$P_{leaving}(k) = \frac{U_{leaving}(k)}{U_{active}(k-1)} * 100 \tag{5.4}$$

Where the $U_{active}(k)$ is the number of active users in week k as calculated by Equation 5.1 and $U_{leaving}(k)$ is the number of leaving users in week k.

Using the matplotlib and numpy packages we visualise these values opposite each other for each week. The first two weeks and last three weeks of the Telegram group data will be omitted from the visualisation, as well as the first and last three months of the Darknet marketplace data.

The average percentage of new and leaving users is calculated for both the Darknet marketplaces and Telegram groups using the mean method. In the case where mul-

tiple averages are combined each of the Telegram groups and Darknet marketplaces is given the same weight.

5.4.4 Advertisements

To visualise the development of the number of advertisements over time we gather the number of advertisements for all marketplaces in the datasets per week.

In the case of the three Darknet marketplaces, we look at the publishing date of each of the item listings on the marketplace. The advertisements are grouped per week and summed to get the number of listings for each week the marketplace was operating.

Before the messages in the Telegram groups can be grouped by week, the non-advertisements must first be filtered out. This is done using the classifier explained in Section 5.3.2. The classifier is used to determine if each of the messages in a Telegram group during the measurement period is an advertisement or a non-advertisements. For all advertisement messages the date and time the message was posted is saved. The advertisements are then grouped by publishing week and a count is generated for the total number of advertisements each week.

Chapter 6

Organisational Structure

In the following chapter we will look at the differences and similarities in organisational structure for the Darknet marketplaces and Telegram. First, we will look into the administrators and owners of the marketplaces in Section 6.1. Next, in Section 6.2 we will look at the different ways the marketplaces are moderated and what systems are in place to help with this. Lastly, in Section 6.3 look into the different payment methods offered and used for orders on both marketplaces.

6.1 Administrators

Both types of marketplaces do not run fully autonomously. There are a number of matters that are handled by users working on or for the marketplaces. Firstly, we will look at the administrators and owners of the marketplaces.

Darknet Marketplaces

Table 6.1 show the number of administrators according to the user type in the three darknet marketplaces. Whilst the administrator users for Hansa and Wallstreet appear to be actual users, the admin users for Alphabay are two users with usernames ‘Admin’ and ‘Support’. We believe that these are general accounts and therefore not linked to a singular person.

The Alphabay dataset has different User Groups next to the User Type values that each user has. There is an Administrator group containing the 2 admin users, next

Marketplace	**Number Users with Admin/Founder User Type**
Wallstreet Market	3
Hansa Market	4
Alphabay Market	2

Table 6.1: Darknet Marketplaces staff based on User Type

Marketplace	**Minimum number of staff**
Wallstreet Market	4
Hansa Market	4
Alphabay Market	11

Table 6.2: Darknet Marketplaces combined minimum number of staff

to which there are also 'Moderator', 'Manager' and 'Public Relations' groups. The Moderator group contains 7 users, the Manager group contains 1 user that is also a member of the Moderator group. The Public Relations group also contains 1 user. Therefore, there are a minimum of 11 user accounts that appear to be the staff that ran Alphabay Market.

Wallstreet Market only has a 'Buyer' and 'Seller' User Group, so no extra information on the staff running the marketplace can be found there. However, when looking at the support tickets that are created for the handling of disputes there are admin notes attached to the support tickets. All these admin notes originate from a single user account which does not have the User Type Admin/Founder, but 'Deleted'. Therefore, there are a minimum of 4 user accounts that appear to be the staff that ran Wallstreet Market.

Table 6.2 shows the minimum number of staff accounts that are used for each of the three marketplaces. As there is no further data in the dataset on for example which user resolved disputes, we cannot say with certainty that these are the only staff members. There might be more staff members that were classified as normal users by their User Type and were not placed in a User Group. There might also be more persons having access to a singular account which is used for admin tasks. Our results are therefore a lower-bound to the number of administrators/staff in each of the groups.

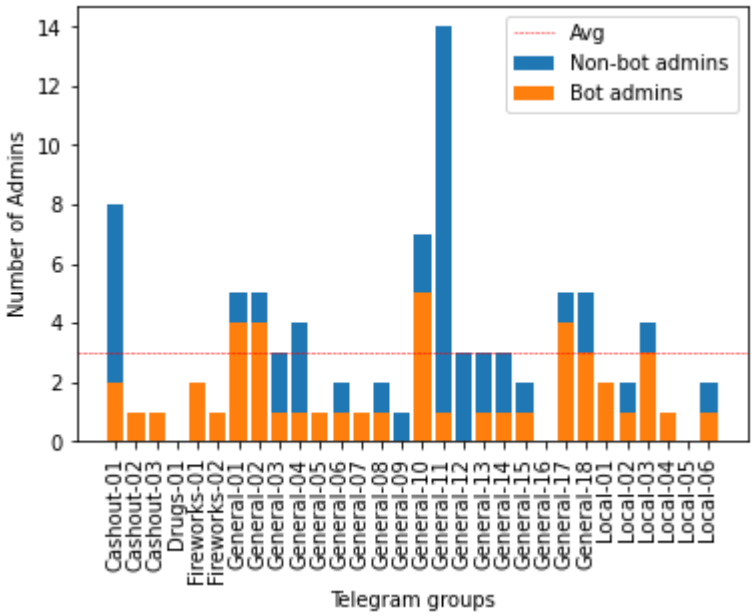


Figure 6.1: Number of visible admins per Telegram Group

Telegram

As elaborated on by Section 5.1.1, we will specifically look at the users in the Telegram group user list that have a specific title. Figure 6.1 shows the total number of visible admins, split up into bot and non-bot admins, for each of the Telegram groups. There are three groups (Drugs-01, General-16 and Local-05) that have no visible administrators at all. A few groups only have visible admins that are bots: Cashout-02, Cashout-03, Fireworks-01, Fireworks-02, General-05, General-07, Local-01 and Local-04. Groups General-09 and General-12 are the only two groups that contain only visible admins that are not bots.

On average, a Telegram group has 3 visible administrators, out of which 2 are bots and 1 is a non-bot administrator. Figure 6.1 shows a few groups that have a number of administrators that is much higher than average: Cashout-01 and General-11. What can be seen by the graphs of both these groups is that the larger portion of the administrators are non-bot admins.

Comparison

When we compare the number of administrators for the Darknet marketplaces with that of the Telegram groups we see that there is not much difference in the numbers. The minimum number of staff for the three Darknet marketplaces is slightly higher

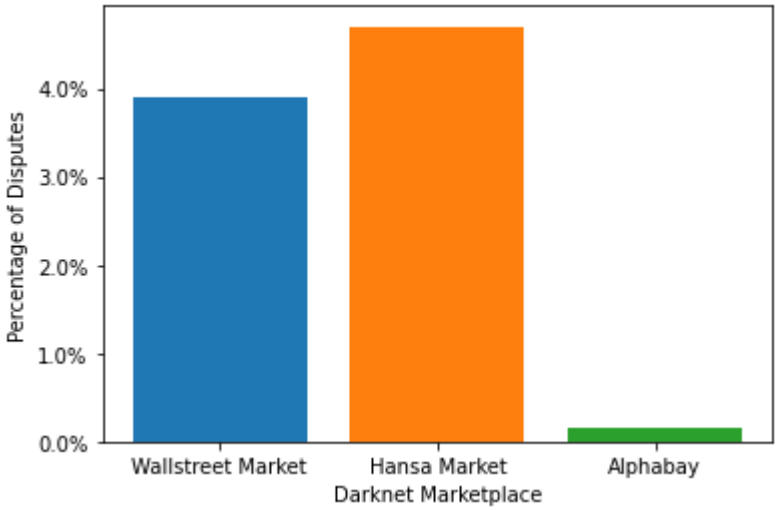


Figure 6.2: Percentage of Disputes out of all orders per Darknet Marketplace

than the average minimum number of administrators for the Telegram groups. One big difference is in the usage of bots. Almost all Telegram groups rely on the use of bots to make the managing of the group easier and to automate some processes. A directly similar thing to bots does not exist on the Darknet marketplaces as most of the functions these bots automate are already part of the marketplace mechanism itself.

6.2 Marketplace Moderation

There are a number of ways in which the different marketplaces are moderated. Next to this the marketplaces also make use of different systems such as dispute handling, feedback ratings and Telegram bots that are used to improve the user experience on the marketplace. Users on the Darknet marketplaces have the possibility to open disputes on orders and to give feedback to the sellers of items they have bought. Telegram groups make use of bots to manage the workings of the groups.

Darknet Marketplaces - Disputes

Figure 6.2 shows the percentage of orders that end up being disputed for all three Darknet marketplaces. In total there are 820.491 orders in the Wallstreet Market dataset. There are 31.904 order disputes, so roughly 3,8% of transactions on Wall-

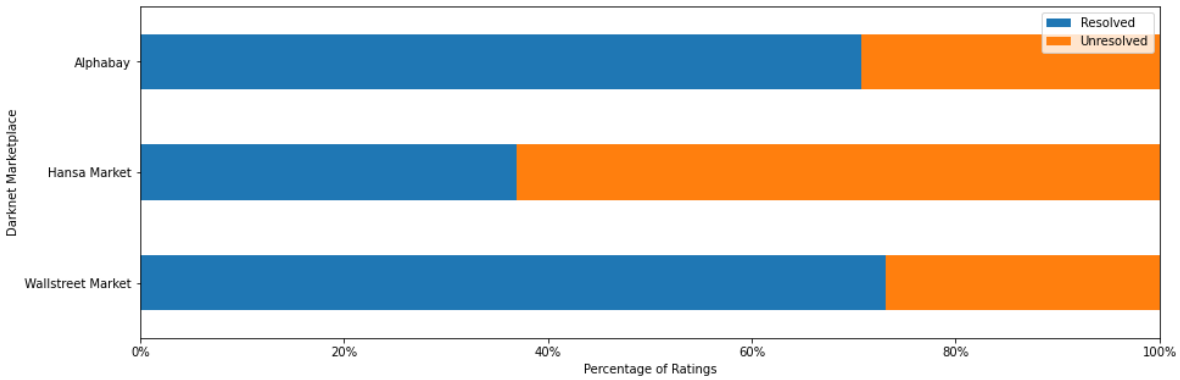


Figure 6.3: Percentage of Resolved/Unresolved Disputes per Darknet Marketplace

street Market ended up in a dispute. There are 160.971 orders in the Hansa Market dataset, out of which 7.558 are disputed. Therefore, 4,7% of the orders ended up in a dispute on Hansa Market. Out of the 10.526.481 orders in the Alphabay dataset, 15.341 are disputed, which accounts for 0,15% of all orders. Compared to the percentage of disputes on Wallstreet Market and on Hansa Market, the percentage of disputes is much lower on Alphabay. The total number of disputes on Wallstreet Market is higher than the total number of disputes on Alphabay, despite the number of orders on Alphabay being more than 12 times bigger.

The percentage of resolved and unresolved disputes can be seen in Figure 6.2. A portion of the disputes on Wallstreet Market was resolved by the moderator staff of the marketplaces and either ruled in favour of the seller or buyer. Out of 31,904 disputes, 23,339 were resolved which is roughly 73,15% of all disputes. The remaining 26.85% of disputes remain unresolved at the time of the marketplace shutdown. Out of all the disputes on Hansa Market, 36,91% were resolved. The other 63.08% of the disputes was left unresolved at the time of the market shutdown. Alphabay has a similar percentage of solved disputes compared to Wallstreet Market. Around 70% of the disputes on Alphabay have been resolved, which amounts to 10.852 disputes. The other 4.489 disputes were still unresolved when the marketplace was shut down.

Whilst both Wallstreet Market and Alphabay have resolved more than half of the disputes, this is not the case for Hansa Market. The percentage of resolved and unresolved disputes for both Wallstreet Market and Alphabay are similar. However, when also taking into account the number of disputes and the percentage of disputes out of all orders we see that Wallstreet Market has the largest number of solved disputes. Hansa Market has both the highest percentage of disputes and the highest percentage of unresolved disputes.

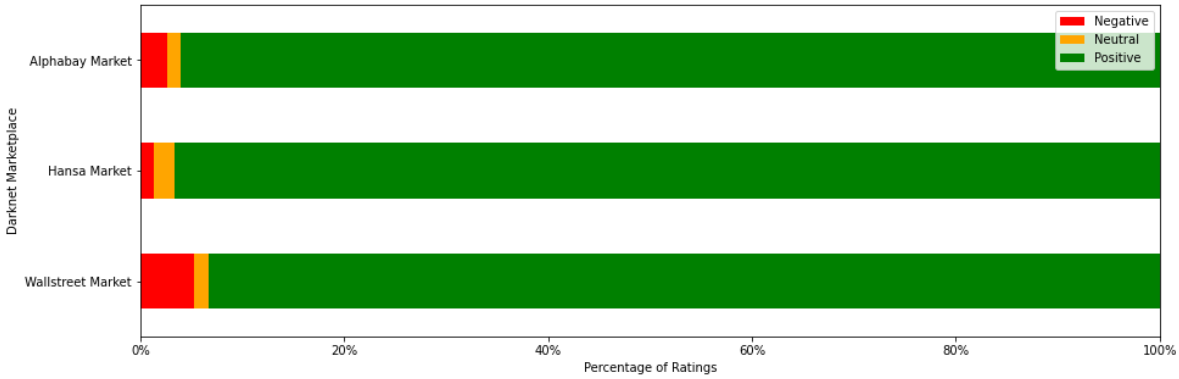


Figure 6.4: Distribution of positive, neutral and negative ratings for the Darknet Marketplaces

Darknet Marketplaces - Feedback System

Using the classified ratings for all three marketplaces as described in Section 5.1.2 we show an overview of the percentage of ratings for each of the three marketplaces in Figure 6.4.

In the case of Wallstreet Market, the rating scheme was between 1 and 5 stars. In total buyers have left feedback on an order 324.653 times. Most of the feedback was a 5-star rating, which accounted for 285.620 ratings. Users left a 4-star rating 17.277 times, whilst 3- and 2-star ratings were left 4.563 and 2.944 times respectively. Lastly, the lowest possible rating given to a seller, 1-star, was given 14.249 times. Therefore, 93,29% of ratings on Wallstreet Market are positive. Out of all ratings 5,29% were negative, and the final 1,41% were neutral ratings.

Out of the 258,250 times buyers have left feedback on their orders on Hansa Market, 249.669 were positive ratings. These positive ratings amount to 96,68% of all ratings. Negative ratings were left 3.592 times whilst buyers gave neutral feedback 4.989 times. In terms of the total number of times buyers left feedback this amounts to 1,39% and 1,93% respectively.

Alphabay only allowed 1-, 2 and 3-star ratings on their orders. In total buyers left feedback 2.823.298 times on Alphabay. The largest portion of these ratings were 3-star ratings: 2.712.200. Ratings of 1 and 2 stars were only given 76.064 and 35.034 times respectively. Therefore, 2,69% of all ratings on Alphabay are negative ratings. Additionally, 1,24% of ratings are neutral and the remaining 97,06% of all ratings are positive.

When we compare the ratings of all three darknet marketplaces with each other, we

see that positive ratings make up the largest portion of all ratings. More than 90% of the ratings for each of the three marketplaces are positive. Wallstreet Market has the largest percentage of negative ratings, whilst Hansa Market has the largest percentage of positive and neutral ratings. The smallest percentage of negative feedback ratings was left on Hansa Market. Overall, vendors on Hansa Market are rated the best whilst vendors on Wallstreet Market are rated the worst out of the three marketplaces. However, these percentages differ only slightly and are overall still small. When we look at the negative ratings on Wallstreet Market, we see that most of the negative reviews state that the seller is a scammer. Therefore a reason for Wallstreet Market having the most negative reviews could be that scammers are removed and banned less quickly than on Hansa Market and Alphabay. The reason for Hansa Market having the highest percentage of neutral and positive ratings can be explained by the fact that Hansa Market is the smallest market out of the three, and is therefore for example not as attractive to scammers as the bigger markets such as Wallstreet Market and Alphabay.

A key point that stands out from the feedback systems on all three marketplaces is that a very large portion of the feedback is positive. This is very different from non-criminal online marketplaces such as eBay and Amazon, as people are usually more inclined to leave feedback if they have a negative experience compared to a positive experience [68].

Telegram - Bots

Figure 6.5 shows the number of bots that have sent at least one message over the duration of the measurement period for each of the Telegram groups. On average, a group has 3 bots that are used to help run the group. Some groups that have a larger number of bots, such as General-04, Drugs-01 and Fireworks-01. However, there are also groups that do not contain any bots that sent messages, such as General-05, General-11, General-12, Local-04 and Local-05. The actual number of bots in the groups might be higher as there could be bots that help manage the group that do not send any messages, in which case they are not noted in this graph.

When we compare the information in Figure 6.5 with that in Figure 6.1 which shows the number of bot admins per group we see that there are some differences. For example, group Cashout-01 is shown to only have 2 bot administrators, but there are 7 bots that send messages. Another example is group Local-04, which is shown to have one bot admin, but has no bots that send any messages. There are two reasons for this: bots can also send messages without having to be administrators

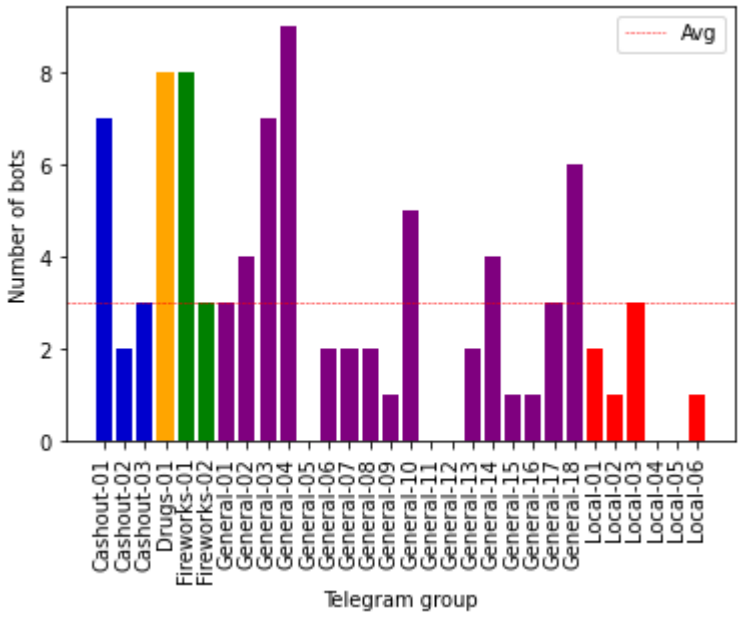


Figure 6.5: Number of bots per Telegram Group

in the group and bots do not necessarily need to send messages in order to help with managing the group. Therefore both figures can show a different number of bots.

Figure 6.6 shows the percentage of messages sent by bots for each of the Telegram Groups. On average, bots account for 5,87% of the messages in groups. Group General-01 is the outlier in this case, as bot messages represent more than 34,36% of the total messages in this group. All other groups contain a considerably lower percentage of bot messages. There are also a few groups that do contain bots that send messages, but these bots send so little messages that their share of the total percentage of messages is less than 0,005%. This is the case for the bots in groups General-09, Local-01, Local-02 and Local-06.

Noticeable is the fact that many groups tend to use the same bots to manage the group. Figure 6.7 shows all the bots that are used in more than 1 Telegram group. Bot-01 is the most used bot, which is used in over 50% of the Telegram groups. Most of these bots are relatively well known group management bots that are used in a large number of non-criminal Telegram groups as well.

Comparison

The above results show that there are a few differences in how both types of marketplaces are moderated and what tools are used. The Darknet marketplaces offer

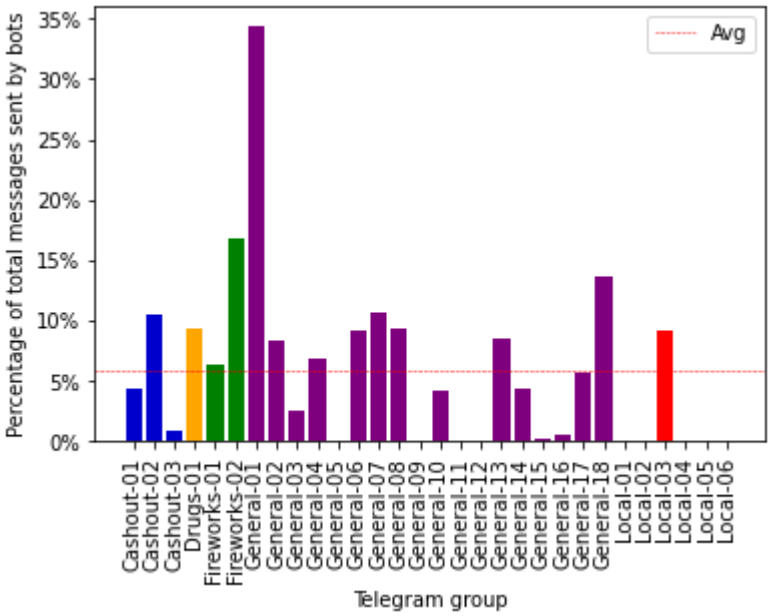


Figure 6.6: Percentage of messages sent by bots per Telegram Group

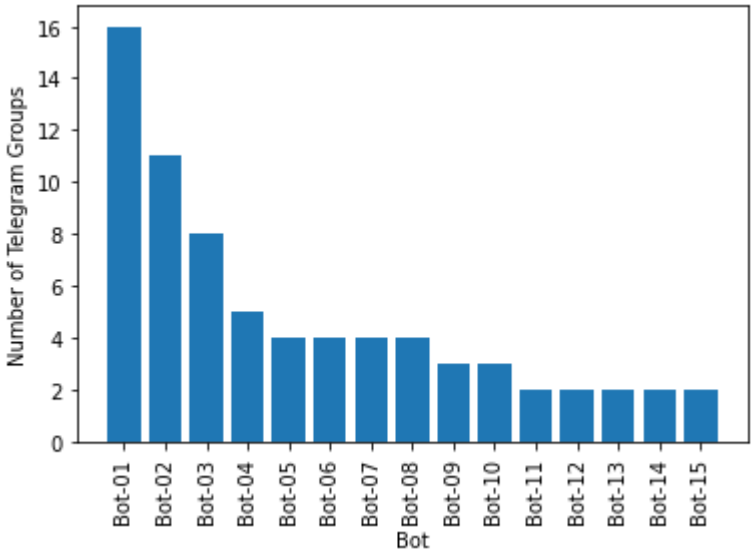


Figure 6.7: Number of Telegram Groups using the same Bots

their users more systems to help in the order process, whilst this is not the case in the Telegram groups. Users on the darknet marketplaces can create a dispute when an order is not received or something is wrong with the product. Next to this they also have a set system which they can use to give feedback on a seller. This is not streamlined in the case of Telegram groups, as these groups are mostly used for the advertisement of goods and services but when a user wants to buy a product they need to contact the vendor directly through a personal message. Therefore the entire ordering process is removed from the marketplace, leading to these marketplaces not handling disputes between buyers and sellers. Users do have the opportunity to write feedback messages in the Telegram group, but there is no centralised place where all feedback can be gathered on all sellers. Therefore, Telegram is less organised in terms of feedback which makes it more difficult to monitor for both the users and sellers. In the case a user wants to buy an item advertised via Telegram, there is no direct way to see feedback on the seller. Should the user want feedback on the seller they either have to look back at all the messages in the group to see if another buyer has left feedback, or ask members of the group through a message if anyone has experience in buying from that specific seller.

Next, the bots that Telegram groups use to manage the groups compare to some functionalities that are built into the Darknet marketplaces as well. An example of this are the banlists where users exhibiting unwanted behaviour are placed and removed from the group or marketplace. Therefore, almost all functionalities that the Telegram marketplaces have are also present in the Darknet marketplaces. The only exception to this being the chat functionality in Telegram that allows users to send messages in the Telegram groups, which is not specifically present in the Darknet Marketplaces. However, most Darknet marketplaces do have a separate forum next to the marketplace which serves the same functionality.

6.3 Payment Methods

Darknet Marketplaces

When we look at the possible payment methods on the three Darknet marketplaces we find that whilst the prices of items are usually shown in Euros of US Dollars, all items need to be paid for using different cryptocurrencies.

Table 6.3 shows for each of the three Darknet marketplaces what payment options were available to pay for listings, and what percentage of listings allowed for pay-

	Wallstreet Market	Hansa Market	Alphabay
Bitcoin (BTC)	99,40%	100%	99,97%
Monero (XMR)	60,90%	-	69,69%
Litecoin (LTC)	52.15%	-	-
Ethereum (ETH)	-	-	69,60%

Table 6.3: Payment Method Possibilities in Darknet Marketplaces listings

ment using this specific payment method. From this Table we see that there are four cryptocurrencies used to perform payments on the three Darknet marketplaces. The most common out of the four is Bitcoin, as all three marketplaces allowed for the payment in Bitcoin. Hansa Market uses only Bitcoin and did not allow any other cryptocurrencies as payment. Litecoin was only used as a payment method on Wallstreet Market, whilst Ethereum was only used as a payment method on Alphabay.

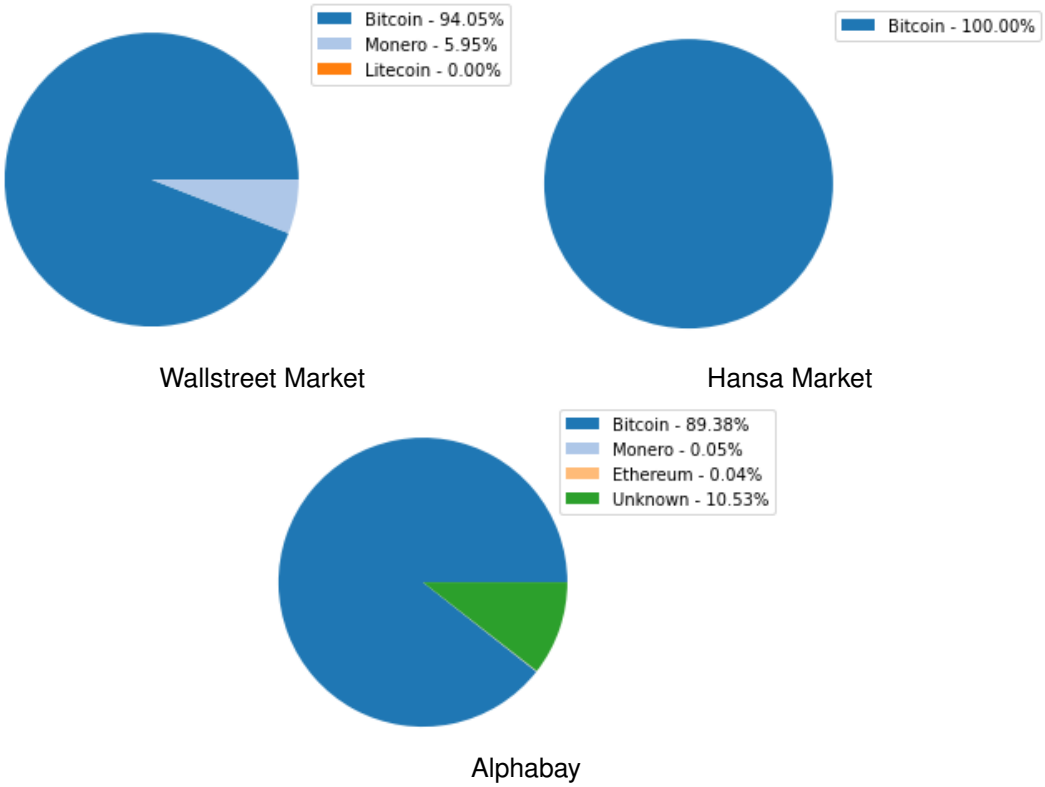


Figure 6.8: Percentage of payment methods used per Darknet Marketplace

Figure 6.8 shows the distribution of payment method over the actual orders. Here we see that whilst there are other payment options available, most of the payments are done using Bitcoin. Though Litecoin is available as a payment method for selected items on Wallstreet Market, the actual payments made with Litecoin represent less than 0.005% or all payments. Similarly, both Monero and Ethereum combined make

up less than 1% of all payments on Alphabay. For 10,53% of the orders on Alphabay, it is unknown which payment method is used. We believe that the reason the most payments are made using Bitcoin is because it is the most well-known cryptocurrency and can easily be bought using a number of different online cryptocurrency exchanges, which is not always the case for the lesser-known cryptocurrencies.

Next to this all three Darknet marketplaces make use of a multisig escrow where the payment for a listing is first being held by the marketplace. If the buyer has received the item the payment is released to the seller. This allows for the creation of disputes as elaborated on earlier in this Section, as well as more security in the ordering process.

Telegram Groups

As the ordering process through Telegram groups is mostly done outside of the groups not much is known about the payment methods. Some advertisements contain the prices for the product that is being advertised. However, most of the advertisements only contain information on the products to be advertised and no prices or payment methods. These messages usually state that if a party is interested in buying the products that they should contact the seller directly via a private message.

In the messages that do have a requested payment method present there are a large number of different options on payment methods. A number of cryptocurrencies can be found as requested payment methods, such as: Bitcoin, Ethereum, Litecoin, Monero. Payment through PayPal, PaySafe or iDEAL is also often stated as a possibility. Next to these 'normal' payment methods a range of numerous other methods can also be seen, such as crypto vouchers or Bol.com giftcards.

Comparison

When comparing the payment processes for orders on the Darknet Marketplaces and Telegram groups there are some big differences. The entire ordering and payment process for items on the Darknet Marketplaces is done through the marketplace itself, using an escrow service to secure the payment as well as having a set number of payment options. On the other hand, sales made through advertisements on the Telegram groups are usually handled outside of the group in private messages. This allows for a bigger range of payment methods tailored to each individual seller, but also poses a higher risk as no escrow services is used. Next to

this a number of payment methods advertised on the Telegram groups are relatively easy to trace back to individuals, such as iDEAL or Paypal. On the contrary the Darknet marketplaces only use cryptocurrencies as payment methods for an extra layer of security.

Chapter 7

Users

Here we describe the results on the investigation on the differences between the usage of the traditional digital criminal marketplaces and that of emerging digital criminal marketplaces on Telegram by their respective users. We first look at the total number of users in Section 7.1. Next, we look at the number of active users in Section 7.2. Finally, the division of sellers and buyers will be compared in Section 7.3.

7.1 Number of Users

We compare the total number of users for both the Darknet marketplaces and the Telegram groups. This subsection specifically focuses on the absolute number of users and not on the activity level of the users.

Darknet Marketplaces

Figure 7.1 shows the total number of unique users in each of the three Darknet marketplaces. Both Wallstreet Market and Alphabay have more than a million users each. Alphabay is the largest of the three, with 1.859.973 users. Wallstreet Market has 1.150.842 user accounts. Hansa Market is the smallest of the three, having only 420.274 users in total.

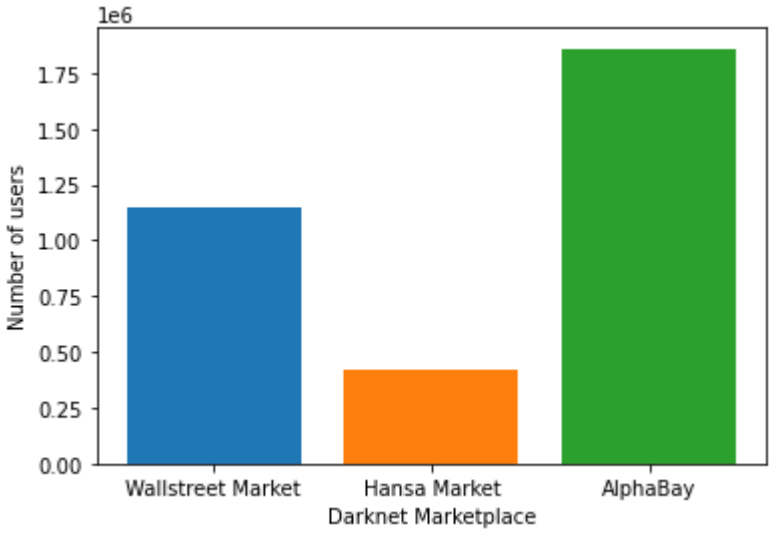


Figure 7.1: Number of unique users per Darknet Market

Telegram Groups

Figure 7.2 shows the number of unique users in each of the Telegram groups. Each colour in the graph represents a different group focus. We can see that there are two groups that have more than 8000 users: General-11 and General-03. There are also two groups that have less than 1000 users, Cashout-03 and General-16. The red dotted line in the Figure shows the average number of users of all groups: 3569,7. The actual number of users in these groups, including the users that do not send any messages is assumed to be higher. Unfortunately, data on users that do not send messages in the groups is not present in the dataset and therefore we cannot draw any conclusions about this.

Figure 7.3 shows the average number of users for each of the five categories in which the Telegram groups are sorted. Here we see that overall, the most users are in the Drugs-focused groups. Though there is only one Drugs-focused group in the dataset, so this can give a skewed average. We also see that there are a relatively large number of users in the Fireworks-focused groups.

Comparison

When we compare the total number of users of the Darknet Marketplaces to that of the Telegram Groups we see that on average the Darknet marketplaces are 320 times bigger than the Telegram Groups. These large differences can be partially explained by the fact that the data gathering time period is much larger for the Dark-

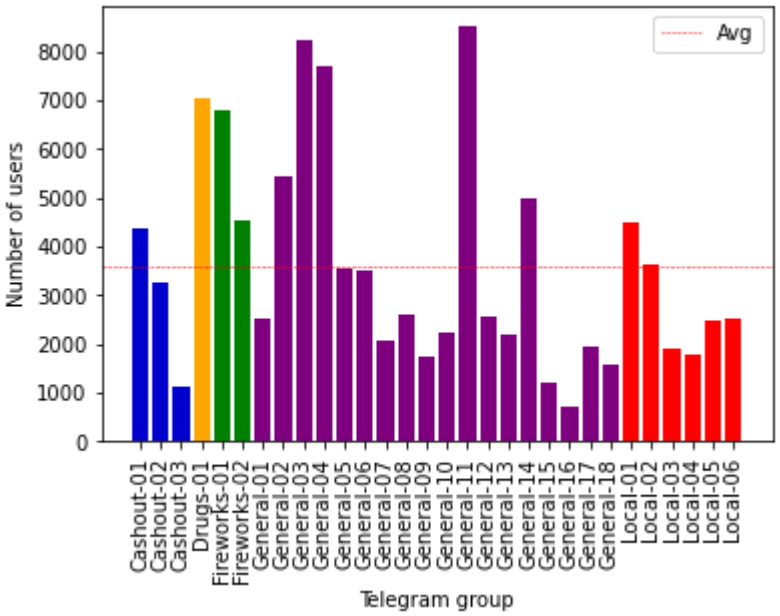


Figure 7.2: Number of unique users per Telegram Group

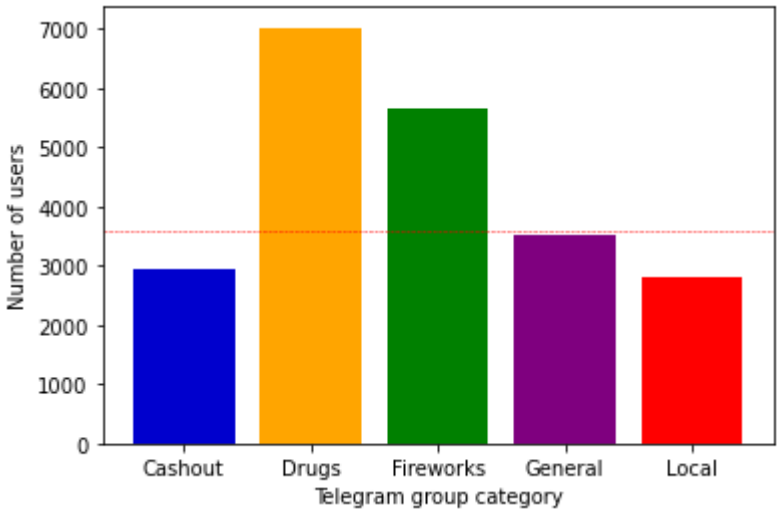


Figure 7.3: Average number of unique users per Telegram Group Focus

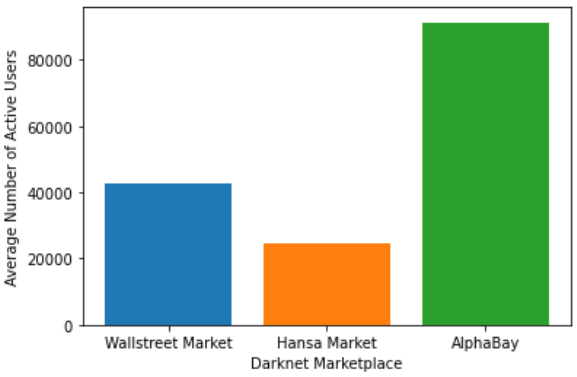


Figure 7.4: Average number of active users per Darknet Market

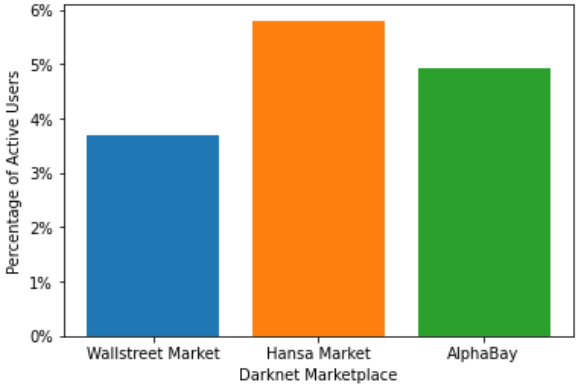


Figure 7.5: Percentage of average active users per Darknet Market

net marketplaces. Next to this, all three of these markets have been known as the biggest criminal marketplace on the Darknet at some point during their operation. Next to this, the Darknet marketplaces are also used by users worldwide, whilst the Telegram groups almost only contain messages in Dutch and are specifically focused on Dutch users.

Most of the times Telegram groups have a specific focus whilst the Darknet marketplaces are a very general marketplace not aimed towards a certain category of services or goods. Therefore, when we combine the number of users for all 30 Telegram groups we get a total of 107.091 users, which is only 4 times smaller than Hansa Market. It is also important to note that the measurement period for the Darknet marketplaces spans multiple years, whilst the measurement period for the Telegram groups only spans a few months.

7.2 Number of Active Users

The total number of users as elaborated on in Section 7.1 gives an overview of how many users have once used the marketplaces. However, not all users use the marketplaces at the same time. Users can join and leave at different points in time. Therefore we also look at the maximum number of active users for each of the marketplaces.

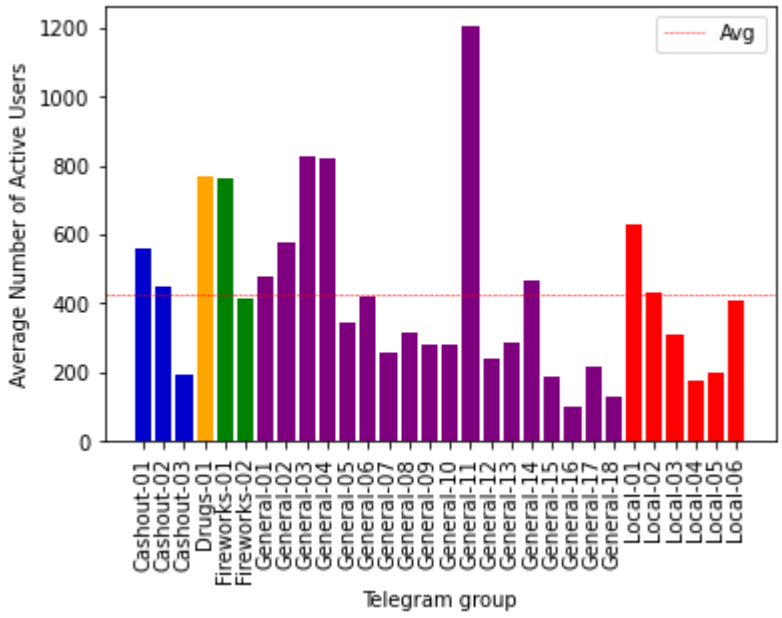


Figure 7.6: Average number of active users per Telegram Group

Darknet Marketplaces

Figure 7.4 shows the average number of active users for the three Darknet marketplaces. An explanation on how these values have been calculated can be found in Section 5.2.2. The percentage of active users compared to the total number of users can be found in Figure 7.5. We see that the largest average number of active users belongs to Alphabay. The smallest average number of active users belongs to Hansa Market. However, these active users account for the largest percentage of the total user base compared to the other two Darknet marketplaces. Therefore, Hansa Market has the largest active user base percentage wise. The average number of active users for Wallstreet Market amounts to the smallest percentage of the total number of users of the three marketplaces: only 3,69%.

The average percentage of active users relative to the total number of users for the Darknet marketplaces is 4,8%.

Telegram Groups

Figure 7.6 shows the average number of active users for all Telegram groups. We can see one clear outlier: General-11, that has a much larger average number of active users compared to all the other groups. There are also a few groups that have less than 200 active users on average: for example groups General-16 and

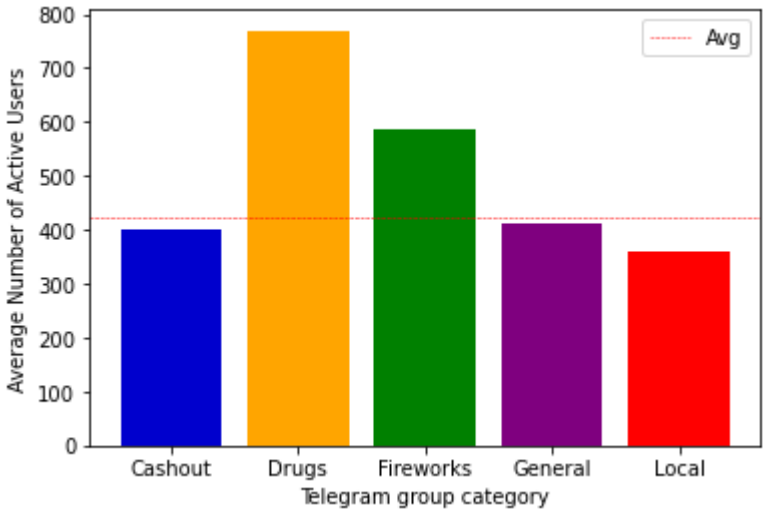


Figure 7.7: Average number of active users per Telegram Group category

General-18. We can also observe that most Local-focused groups have a smaller than average number of average active users compared to all the other groups.

Figure 7.7 shows the average number of active users for the Telegram groups combined by category. This shows that on average, the Drugs- and Fireworks-focused groups have the highest average number of active users. Opposite to this, the Local-focused groups have the lowest average number of active users.

The percentage of active users with regards to the total number of users in the Telegram groups can be found in Figure 7.8. We see that whilst the group General-11 has the highest average number of active users, this number only accounts to less than 10% of the total number of users, making it one of the groups with the smallest active user base percentage wise. No group has less than 8% active users, the average percentage of active users being 12,38%. The highest percentage of active users can be found in group General-01, which has an active user percentage of 19%.

Figure 7.9 shows the average percentage of active users for all five Telegram group categories. When we compare the results in this image to Figure 7.7 we see that the groups that have an above average number of active users have a below average percentage of active users. Groups in the Cashout category have the highest percentage of active users.

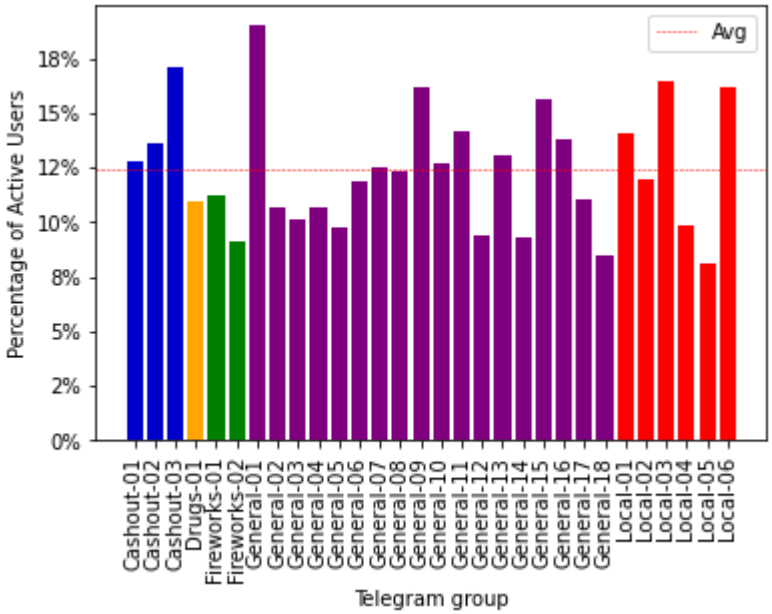


Figure 7.8: Percentage of active users per Telegram Group

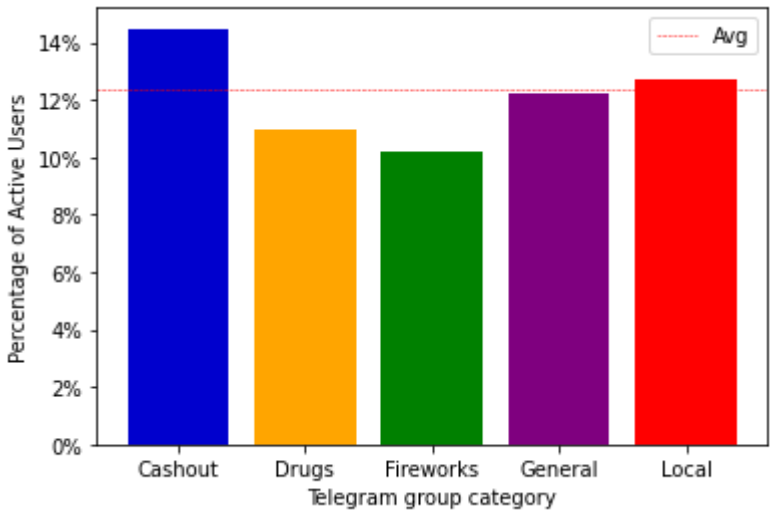


Figure 7.9: Percentage of active users per Telegram Group category

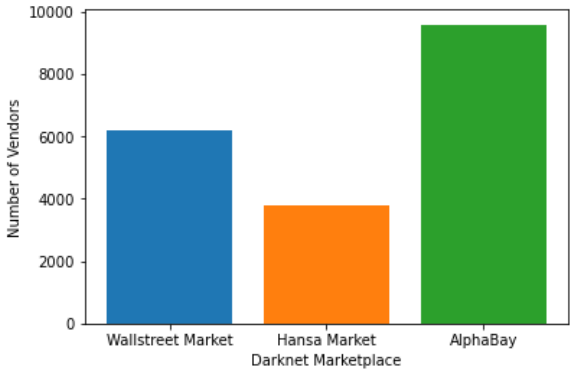


Figure 7.10: Number of Vendors per Darknet Marketplaces

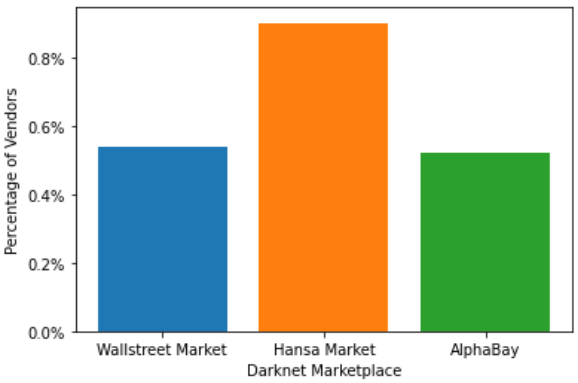


Figure 7.11: Percentage of vendors per Darknet Marketplaces

Comparision

The number of active users is much higher for the three Darknet marketplaces than for the Telegram groups as can be seen by Figures 7.4 and 7.7. However, when we look at the percentage of active users we see that the percentage of active users in Telegram is almost double that of the Darknet marketplaces. This suggests that the users in the Telegram groups engage in a different way than users on the Darknet marketplaces. A possible reason for this could be the difference in other uses of the platforms next to the marketplaces. For example, the Darknet marketplaces are its own entity and have a specific web page users need to navigate to using special software such as a Tor browser. Telegram on the other hand is a messaging app that users have on their phones, which they can also use to access other groups on the app next to the marketplace groups. Therefore, it could be possible that due to users using the Telegram app for other purposes as well, the Telegram marketplaces are more visible and are therefore more actively used by users without a predetermined intention to visit the marketplace.

7.3 Vendors

Darknet Marketplaces

Figure 7.10 shows the number of vendors for each of the Darknet Marketplaces. Alphabay has the most vendors out of all three marketplaces: more than 9.500 vendors. Hansa Market has the least amount of vendors, having only 3.798 user

accounts that sell items on the marketplace.

The percentage of vendors compared to the total number of users for each of the three Darknet marketplaces can be found in Figure 7.11. Here we see that whilst Hansa Market has the lowest amount of vendors, it actually has the highest percentage of vendors. Still, all marketplaces have a percentage of vendors that is smaller than 1% of the total number of users.

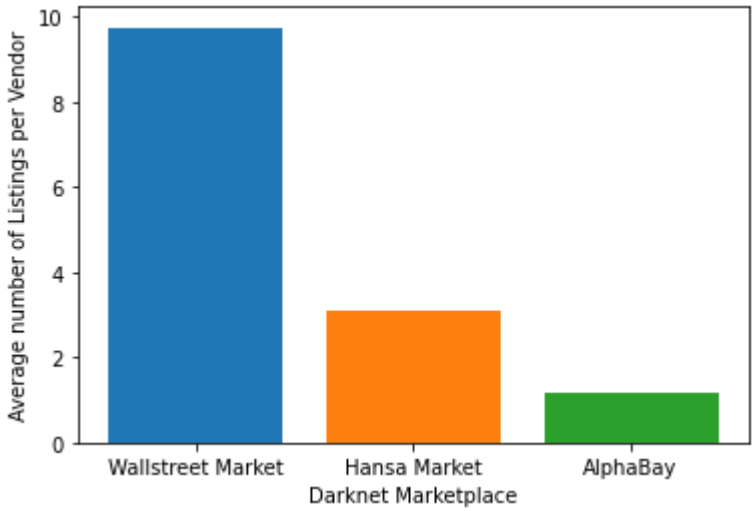


Figure 7.12: Average Listings per Vendor per Darknet Marketplaces

Figure 7.12 shows the average number of listings per vendor on the three Darknet Marketplaces. Here we see that on Wallstreet Market, each vendor has on average almost ten listings. However, vendors on Alphabay only have on average one listing.

Telegram Groups

Figure 7.13 shows the number of vendors for each of the Telegram groups. There are only a few groups that contain more than 5.000 unique vendors: Drugs-01, Fireworks-01, General-03 and General-04. Next to this there are also a few groups that contain less than 1.000 unique vendors. On average, a Telegram group has 2.508 vendors.

The average number of vendors for each of the five Telegram group categories can be found in Figure 7.14. From this overview it can be seen that the Fireworks- and Drugs-focused groups have a relatively high number of unique vendors. The Local-focused groups on average have the least amount of unique vendors compared to all the other categories. A possible reason for this could be that because the Local-focused groups only focus on a very specific city/region, the number of sellers in

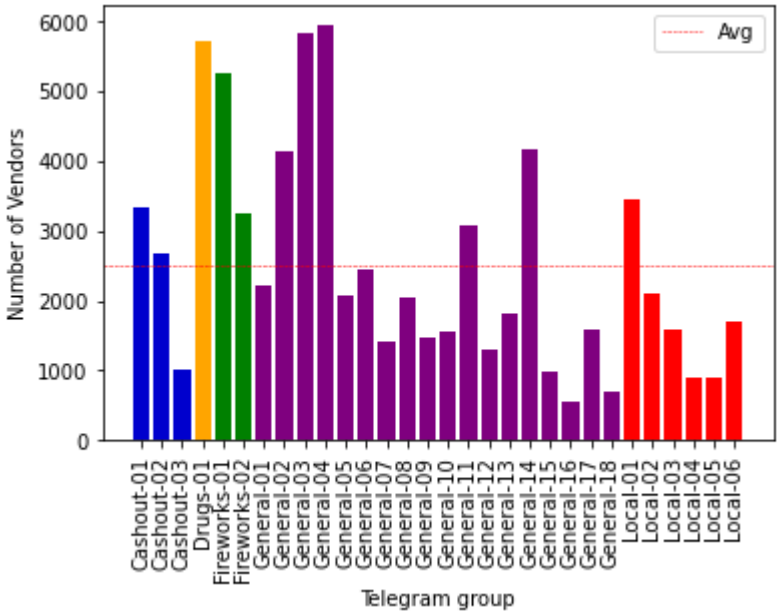


Figure 7.13: Number of Vendors per Telegram Group

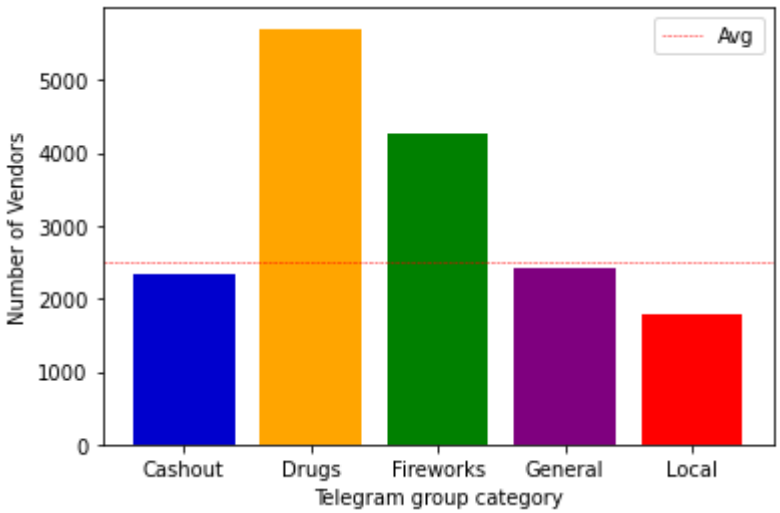


Figure 7.14: Average Number of Vendors per Telegram Group category

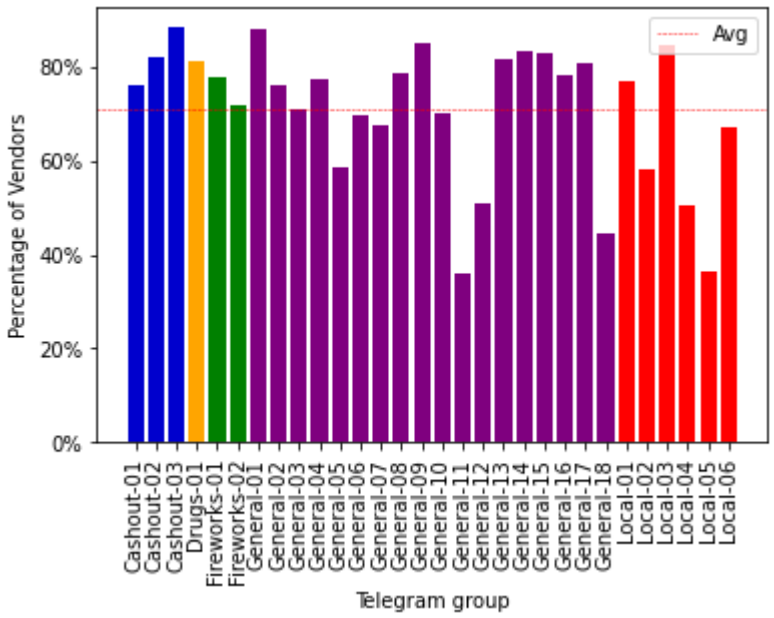


Figure 7.15: Percentage of Vendors per Telegram Group

these regions is smaller compared to the other groups which are country-wide.

Figure 7.15 shows the percentage of vendors out of the total number of users for each of the Telegram Groups. Figure 7.16 shows the average percentage of vendors for each of the five Telegram group categories. On average, 71.12% of the users in the Telegram groups are vendors. There are a few outlier groups that have a much lower percentage of vendors, such as groups General-11 and Local-05. Similarly to the actual number of vendors, the Local-focused groups have a below average percentage of vendors. Overall, the Cashout-focused groups have the highest percentage of vendors of all five categories.

Figure 7.17 shows the average number of listings per vendor for each of the Telegram groups. Figure 7.18 gives an overview of the average number of listings per vendor for each of the Telegram group categories. Only unique advertisements are counted for the calculation of these values. Therefore the total number of advertisements that vendor send might be higher as vendors are able to send the same message multiple times. Overall, the average number of listings per vendor is 18. There are two high outliers who have an average of over 25 unique listings per vendor: General-02 and General-14. The Local-focused groups all have a below average number of listings per vendor whilst all Fireworks-related groups have a higher than average number of listings per vendor.

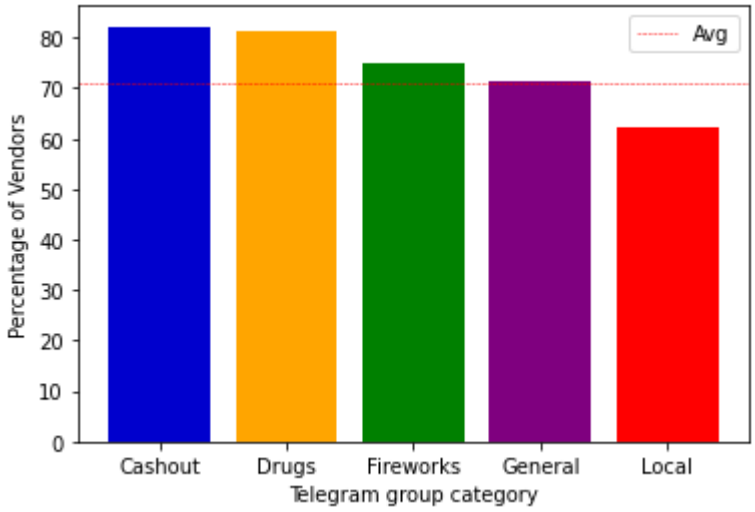


Figure 7.16: Percentage of Vendors per Telegram Group category

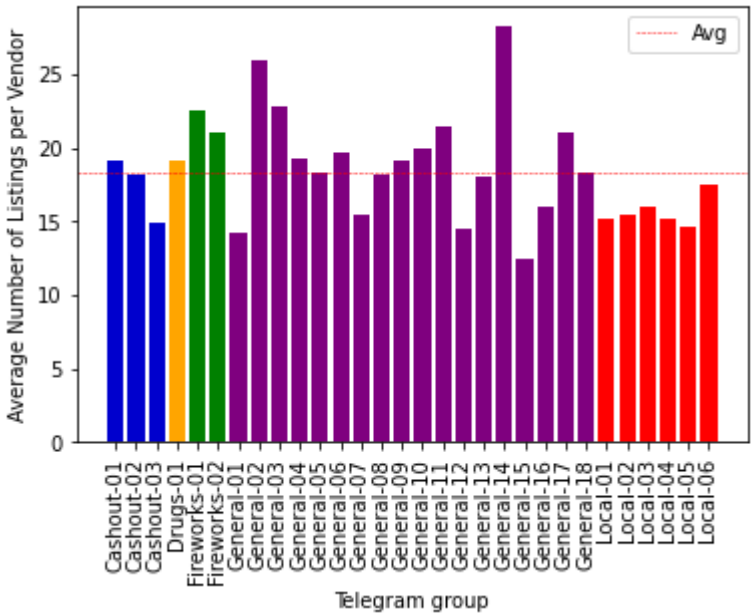


Figure 7.17: Average Number of Listings per Vendors per Telegram Group

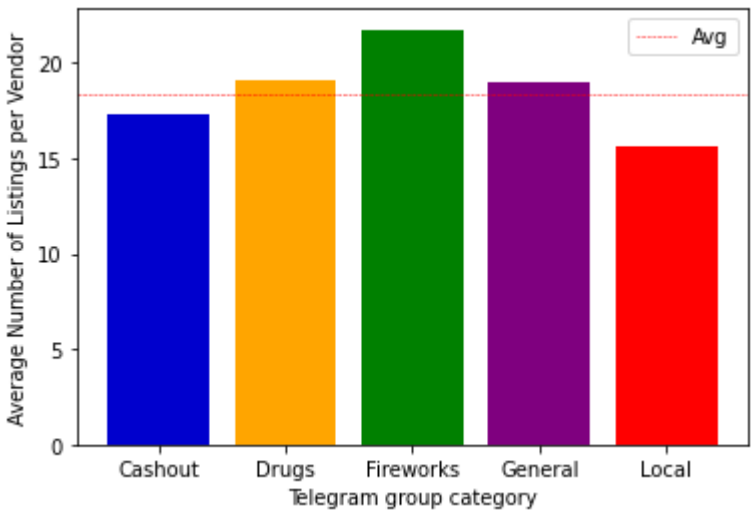


Figure 7.18: Average Number of Listings per Vendors per Telegram Group category

Comparison

When we compare the number of vendors for both the Darknet marketplaces and the Telegram groups we see that in terms of total number of vendors the Darknet marketplaces have a higher number of vendors than the Telegram groups. The only exception to this statement is that the Fireworks- and Drugs-focused groups have slightly more vendors than Hansa Market. However, when we look at the percentage of vendors out of the total number of users we see that the percentage of vendors for the Telegram groups is much higher. Important to note is that the total number of users for the Telegram groups is expected to be higher than the amount being used in the calculations. This is due to the fact that members in the Telegram groups who do not send any message are not registered in the dataset and are therefore not counted towards the total number of users. The average number of listings for vendors in the Telegram groups is also a lot higher than that of vendors on the Darknet marketplaces. Wallstreet Market has the highest average number of listings per vendors however the average listings per vendor is higher for all Telegram groups analysed.

Chapter 8

Goods & Services

In this chapter we try to answer the research question ”What are the differences in types of goods and services being advertised on traditional criminal marketplaces and emerging digital criminal marketplaces on Telegram?”. In Section 8.1 we look at the advertisements and the distribution of categories of advertisements in the Darknet Marketplaces dataset. Section 8.2 elaborates on the advertisements in the Telegram groups. First we look at what percentage of messages in the groups are advertisements, after which we classify these advertisements into the advertisement categories. Finally, we compare the distributions for the Darknet Marketplaces and the Telegram Groups.

8.1 Darknet Marketplaces

Goods and services advertised on the three darknet marketplaces are sorted into small categories that differ for each of the three marketplaces. For the sake of comparison, both between the marketplaces themselves and the marketplaces and the Telegram groups, goods and services are sorted into one of 11 categories defined in Section 5.3.

8.1.1 All Advertisements

Figure 8.1 shows a graphical overview of the percentage of advertisements in each of the categories for all listings on the three darknet marketplaces. Table A.1 in Appendix A.1 gives a numerical overview of the same percentages.

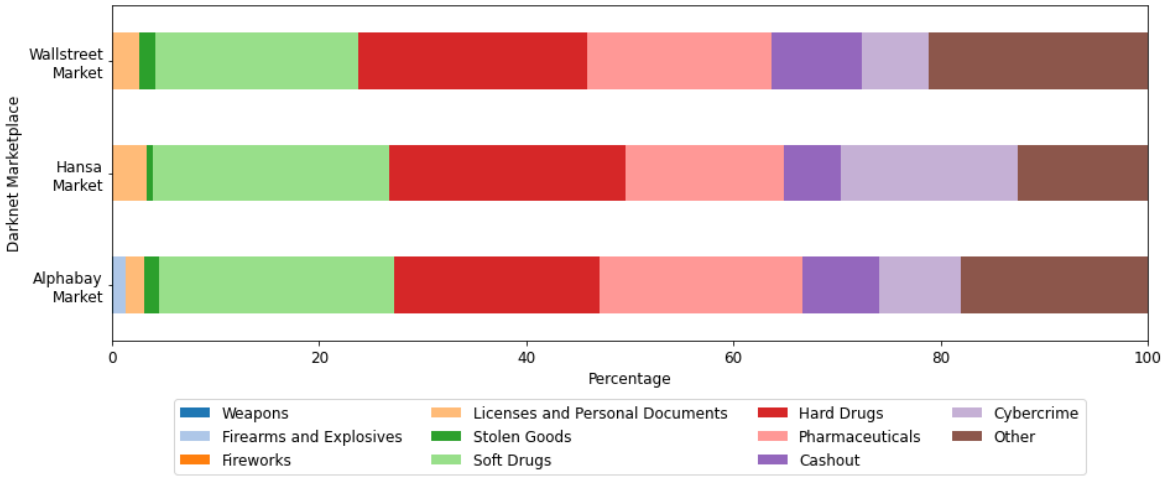


Figure 8.1: Category Distribution of All Advertisements

Out of the 63,711 items advertised on the Wallstreet Market, more than half are either drugs or pharmaceuticals. Most advertisements are for Hard Drugs, whilst there are no advertisements for Weapons, Firearms and Explosives, and Fireworks. The 'Other' category containing all miscellaneous items also accounts for more than 20 % of the total advertisements.

Similarly, the largest part of the items advertised on Hansa Market are either drugs or pharmaceuticals, with Hard Drugs being the most advertised category. Out of the 123,160 items, 17.19 % are advertisements for items related to Cybercrime. There are no advertisements for Weapons, Firearms and Explosives and Fireworks.

In total there are 827,689 advertisements in the Alphabay dataset. Drugs and pharmaceuticals make up for more than half of all these advertisements: 62.2%. All categories are represented in terms of advertisements except for Fireworks.

We observe that compared a relatively large percentage of Soft Drugs is being sold on Hansa Market compared to Alphabay and Wallstreet Market. At the same time, a larger percentage of Hard Drugs is being sold on Wallstreet Market compared to Alphabay and Hansa Market. In total, there are a lot more advertisements on Alphabay than on Wallstreet Market (13 times more advertisements) and on Hansa Market (6.7 times more advertisements). The only market that has any advertisements in the Weapons and Firearms and Explosives categories is Alphabay. None of the marketplaces have any advertisements on Fireworks.

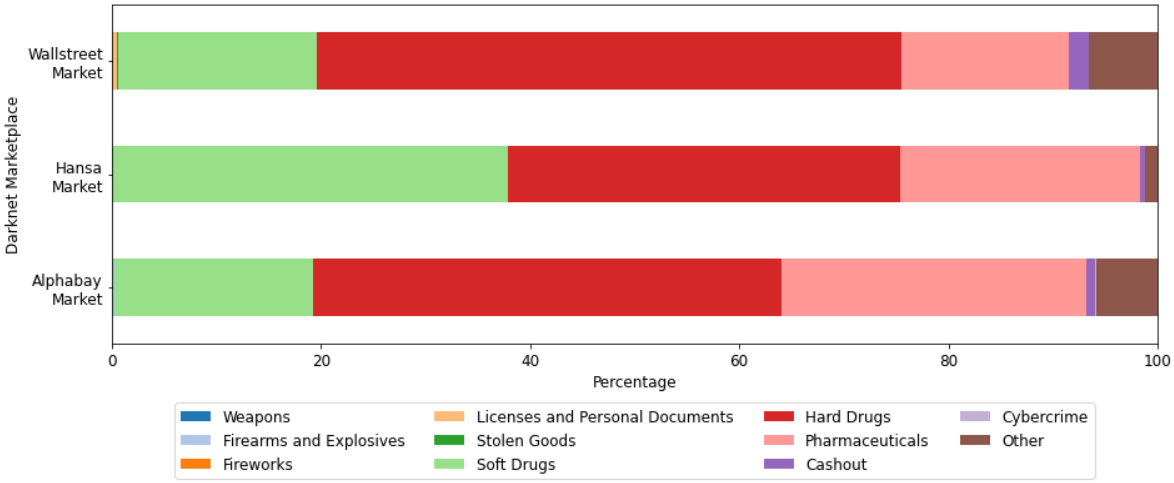


Figure 8.2: Category Distribution of Advertisements Shipping from NL

8.1.2 Advertisements shipping from the Netherlands

All three marketplaces were accessible from anywhere in the world and therefore allowed people from all over the world to buy and sell goods. However, as the goods and services advertised through the Telegram groups are only shipped from the Netherlands, we also look at the advertisements shipping from the Netherlands on the Darknet marketplaces. When we specifically focus on the advertisements originating from the Netherlands, the overview of advertisement categories changes. In this case we only use the Netherlands as the originating shipping location. Figure 8.2 shows the distribution of categories for all items shipped from the Netherlands for the three darknet marketplaces. Table A.2 in Appendix A.1 shows the percentages for each of the listing categories in the three darknet marketplaces.

We observe that more than half of all items shipping from the Netherlands on Wallstreet Market are Hard Drugs. In total there are 2,738 listings that ship from the Netherlands in the dataset, which accounts to around 4.3% of all listings on the marketplace. Next to this, more than 90 % of all items shipped from the Netherlands are drugs of some sort (Soft Drugs, Hard Drugs and Pharmaceuticals). Therefore the percentage of drugs advertisements (both Hard Drugs and Soft Drugs) originating from the Netherlands is much higher than the percentage of the same advertisements in the entire Wallstreet Market dataset. The percentage of Cybercrime advertisements is also much smaller for the advertisements originating from the Netherlands compared to all advertisements. The percentage of Cybercrime advertisements originating from the Netherlands is only 0.02% whilst the Cybercrime category account for 17.19% in the global overview of Wallstreet Market.

In total 7,873 items, roughly 6.4% of the total advertisements, are available to be shipped from the Netherlands on Hansa Market. Hard Drugs, Soft Drugs and Pharmaceuticals make up for more than 98% of these listings. Compared to the distribution of categories for the entire marketplace, there is an increase in percentage for Drugs and Pharmaceuticals, whilst the percentage of all other categories decreases. Some categories, such as Licenses and Personal Documents are no longer present at all.

In the case of Alphabay, 20,923 items are shipped from the Netherlands, which accounts to around 2.5% of the total listings on Alphabay. The largest category of items being sold is Hard Drugs, covering 44.82% of all listings. Compared to the global distribution of categories, the percentage of Soft Drug listings (18.94%) originating from the Netherlands is lower than that in the global distribution. However, the percentage of Pharmaceutical and Hard Drug listings do increase.

Comparing Figure 8.1 to 8.2 we observe that compared to the global distribution, items originating from the Netherlands are largely Drugs or Pharmaceuticals. Other categories are less present, such as Cashout and Cybercrime.

8.1.3 Number of orders

Each listing on the marketplace is available to be bought more than once. Therefore we will also look at the number of orders for each category and compare this distribution to the number of advertisements. Figure 8.3 shows the category distribution for all orders on the three darknet marketplaces. Similarly, Table A.3 in Appendix A.1 shows the numerical overview of the percentages of the same category distribution.

Comparing the distributions for Wallstreet Market, we observe that there are a number of categories that account for a lower percentage of the total orders than the percentage of advertisements. This is the case for listings in the Licenses and Personal Documents, Stolen Goods, Pharmaceuticals, Cybercrime and Other categories. The only two categories that account for a larger percentage of the total orders are Soft Drugs, Hard Drugs and Cashout.

In the case of Hansa Market, the percentage of Cybercrime advertisements is relatively large as noted in Section 8.1.1. However, whilst Cybercrime accounts for 17.19% of the total advertisements on Hansa, it only accounts for 6.72% of the total orders. An increase can be seen for Hard Drugs. Where 22.88% of all advertisements are for items in the category Hard Drugs, 31.54% of all orders are for items

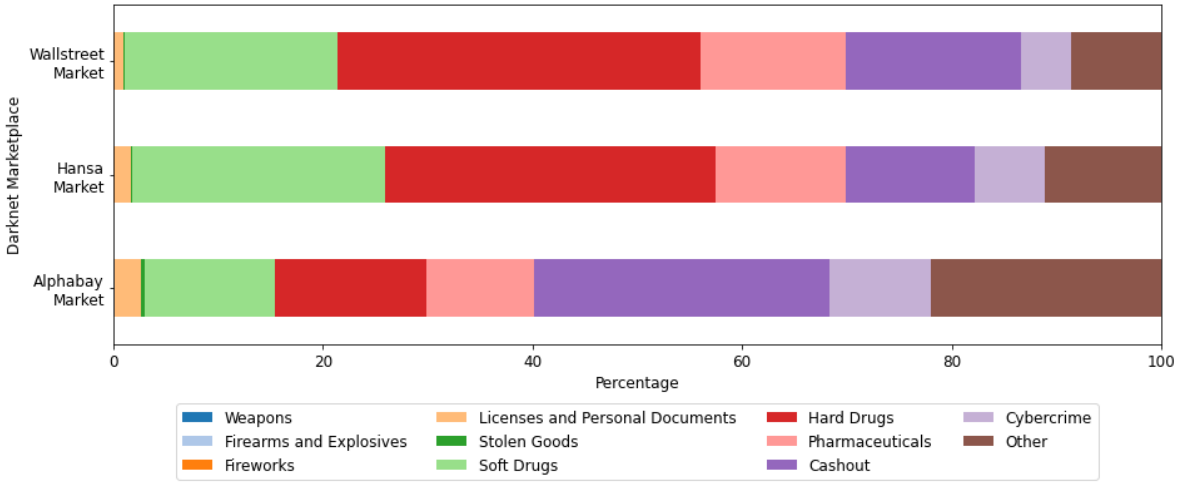


Figure 8.3: Category Distribution of All Orders

in the same category.

When looking at Alphabay, a big difference can be seen in the Cashout category. Items in this category account for 7.32% of all advertisements on Alphabay, but account for more than a quarter of the total orders (28.15%). A decrease can be seen in the Soft Drugs category, where the advertisements in this category account for 22.76% of all advertisements, but the orders only account for 12.41% of the total number of orders. Noticeable is also that Firearms and Explosives account for 1.13% of all advertisements on Alphabay, but their orders only account for 0.09% of all orders.

8.2 Telegram Marketplaces

Using the training dataset and classifier explained in Section 5.3 we classify all the messages in the 30 Telegram groups. Each message will be classified as either an advertisement or a non-advertisement. Advertisement messages are then also classified in terms of their advertisement category.

8.2.1 Advertisements

Figure 8.4 shows the distribution of ads and non-ads over all the Telegram Groups. Table A.4 in Appendix A.1 shows the numerical percentage data for the distribution.

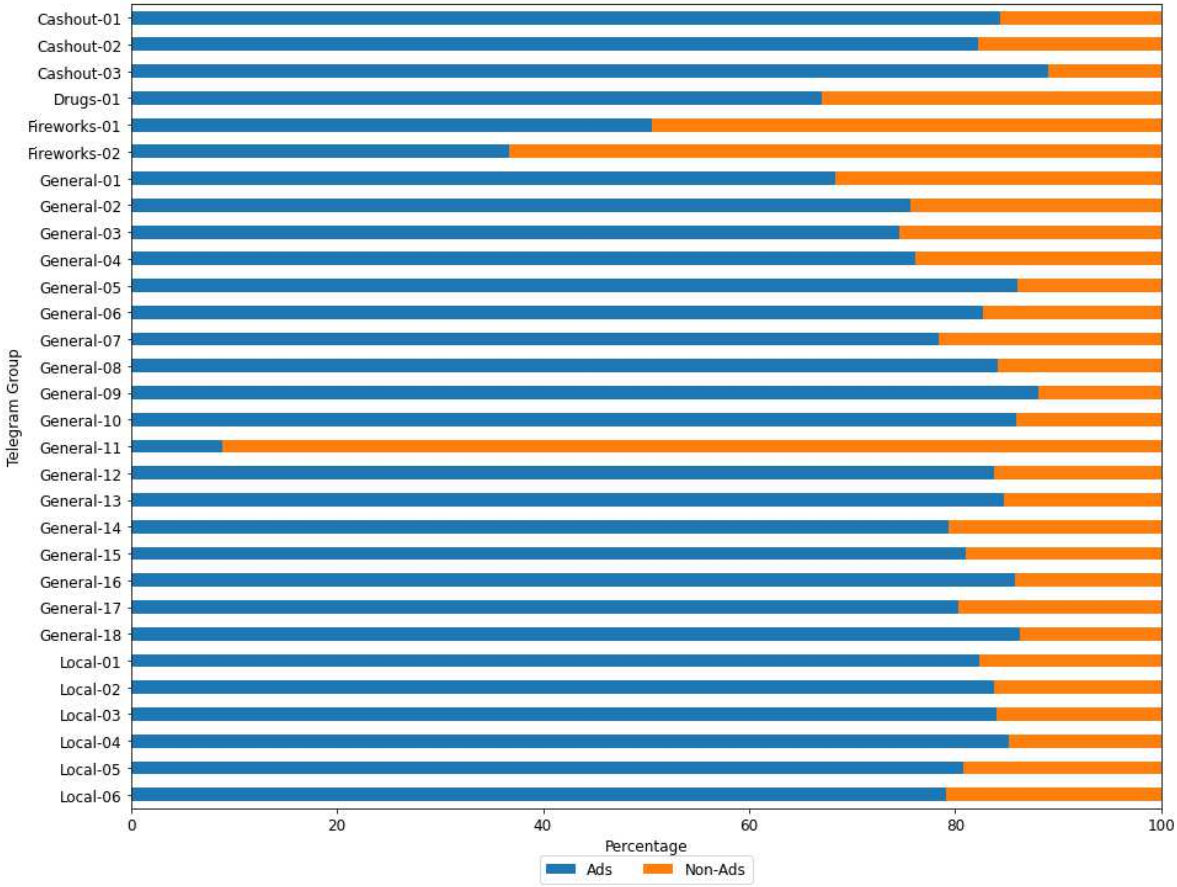


Figure 8.4: Ads / Non-ads distribution over all messages in Telegram Groups

Notable is that in the groups that have Fireworks as a main focus, the percentage of non-advertisement messages is much higher compared to almost all other groups. For both groups the percentage of non-ads messages is around 50% or higher. Another interesting outlier is General-11. This group has the largest percentage of non-advertisements of all groups: around 91%. This is different from all other General groups, as the average percentage of non-ads in all the other General groups is roughly 18,8%

8.2.2 Categories in Individual Groups

Next to classifying if messages are advertisements or not, another classifier is used to classify the category for each of the previously classified advertisements. Information about the classifier and the training dataset can be found in Section 5.3. Advertisement messages are classified into one category by the classifier, depending on the content of the messages.

Figure 8.5 shows the distribution of the 11 categories over all the Telegram Groups. Table A.5 in Appendix A.1 shows a numerical overview of the distribution. Both Fireworks-01 and Fireworks-02 contain a lot of advertisement messages in the Fireworks category, which is to be expected given the main focus of the groups. Out of all advertisements in both groups, around 75% of them are advertisements related to Fireworks. This is a large difference to all the other groups, as they contain less than 1% of advertisement messages categorised as Fireworks advertisements.

Drugs-01 has the largest percentage of advertisements for the Soft Drugs category. However, it does not contain the highest percentage of advertisements in the Hard Drugs category. A number of General groups contain a higher percentage of advertisements for Hard Drugs: for General-02 and General-14 more than 50% of all advertisement messages are Hard Drug advertisements.

Advertisements for Weapons and Firearms and Explosives are almost nonexistent in all groups. The highest percentage of Weapons advertisements is 0.49% for General-18, whilst the highest percentage of Firearms and Explosives advertisements is in Fireworks-02 with 0.84%. The highest percentage of Stolen Goods can be found in General-16, whilst the highest percentage of Licenses and Personal Documents advertisements can be found in General-08.

Pharmaceuticals generally only account for equal to or less than 10% of the total amount of messages for all groups, with the exception of Local-06 and General-

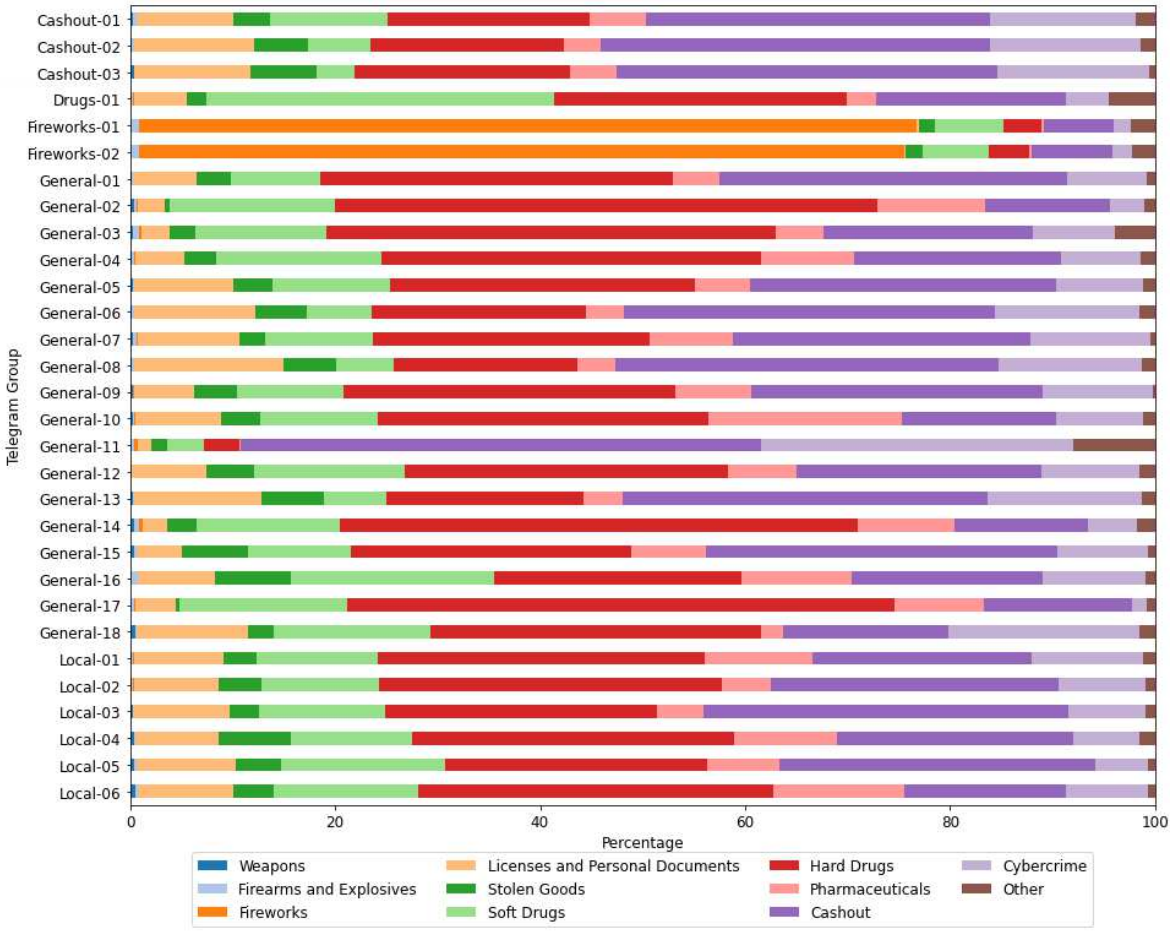


Figure 8.5: Category distribution over all messages in Telegram Groups

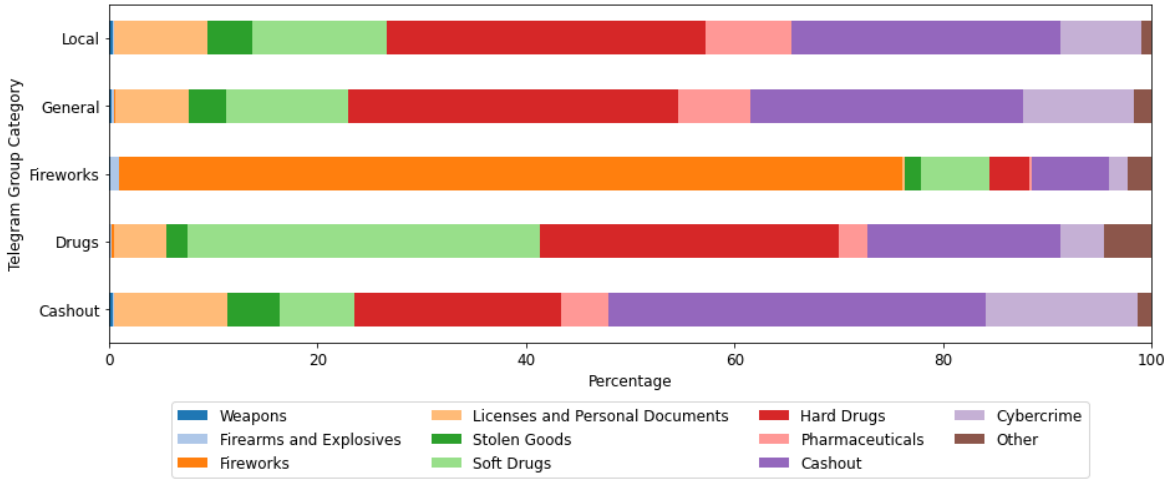


Figure 8.6: Category distribution over all messages in Combined Telegram Groups

10. General-10 contains the largest percentage of pharmaceutical advertisements: around 18,92%. The Cashout category is a category that is more prominent in all groups, with the exception of the Fireworks groups. In the group General-10, more than 50% of all advertisements are Cashout advertisements. Similarly, this group is also an outlier in the category Cybercrime, which account to more than 30% of all advertisements in the group.

8.2.3 Categories in Combined Groups

Figure 8.6 shows the distribution of advertisement categories for each of the different group focuses. Table A.6 in Appendix A.1 shows the numerical overview of the data in the Figure. Over 75% of all advertisements in the Fireworks-focused groups are for advertisements in the Fireworks category, which is clear from the large portion of orange in the Figure. The most advertised category in the Cashout-focused groups is the Cashout category, accounting to 36,21% of all advertisements in those groups. In the Drugs-focused Telegram groups, the most advertised categories are Soft Drugs and Hard Drugs, which combined mark more than 62% of all advertisements in those groups.

The General focused groups and the Local focused groups look very similar. Local focused groups contain slightly more advertisements in the Licenses and Personal Documents category, whilst the General focused groups contain slightly more Hard Drugs and Cybercrime advertisements.

8.2.4 Comparison

In order to do a top-level comparison, we determine the average distribution of categories for all darknet marketplaces as well as all Telegram groups. These distributions are visualised in Figure 8.7, a numerical overview can be found in Table A.7 in Appendix A.1. For this visualisation, the category division for the Darknet marketplaces is taken from Section 8.1.2, only containing the advertisements that ship from the Netherlands. This is done because all advertisements in the Telegram groups also originate from the Netherlands, to therefore get an as accurate comparison as possible.

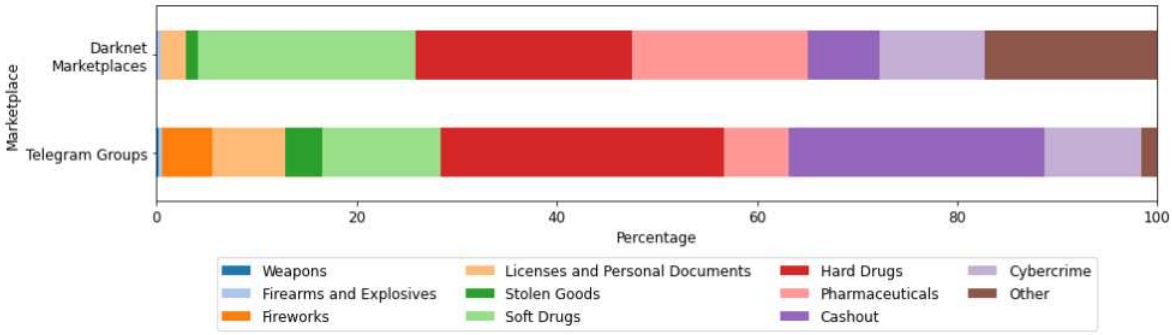


Figure 8.7: Category distribution for overall Darknet Marketplaces and Telegram Groups

Differences between the two types of marketplaces can be see in a number of different categories. Noticeable is that there are no advertisements for Fireworks in the data of the Darknet Marketplaces, whilst there are specific Telegram groups focusing on this category and Fireworks account for roughly 5% of all advertisements. The percentage of advertisements in the Cashout category is also much higher for the Telegram Groups compared to the Darknet Marketplaces: 25,53% and 7,18% respectively. An interesting observation is that the Darknet marketplaces contain a higher percentage advertisements for Soft Drugs and Pharmaceuticals, but the Telegram groups contain a higher percentage of advertisements for Hard Drugs.

The Other category is also much more represented in the Darknet Marketplaces compared to the Telegram Groups. Around 17,24% of all advertisements on the Darknet Marketplaces are Other category advertisements, compared to the 2,14% in the Telegram Groups. There are a few categories where the percentages do not differ greatly from each other, such as the Cybercrime category: 9,70% on Telegram versus 10,51% on Darknet marketplaces. In the case of the Weapons category, we see that the percentage of Weapons advertisements is almost 5 times bigger on Telegram than on the Darknet marketplaces: 0,23% on Telegram to 0,05% on Dark-

net marketplaces. Even though these percentages are small compared to all the other categories, they are still notable. A probable reason for the percentage being much higher on Telegram is that advertisements for Weapons were only allowed to be posted on Alphabay and not on Wallstreet Market and Hansa Market due to marketplace rules. However, the Telegram groups do not have such specific rules and therefore the posting of Weapons advertisements is allowed in those groups.

Chapter 9

Development over Time

In this chapter we answer the research question “How is the usage of both traditional criminal marketplaces and emerging digital criminal marketplaces on Telegram developing over time?”. In Section 9.1 we will compare the number of active users over time, as well as the relative growth and the number of new and leaving users for both types of marketplaces. Section 9.2 focuses on the comparison of the number of messages over time.

9.1 Users over Time

In order to compare the evolution of the Darknet marketplaces and the Telegram groups, we will look at the users of both types of marketplaces over time.

9.1.1 Number of Active Users over Time

The number of active users over time for both the Darknet marketplaces and Telegram groups is calculated by the method described in Section 5.4.1.

Darknet Marketplaces

Figure 9.1 shows the number of active users over time for all three Darknet Marketplaces per week. In terms of the largest number of active members, Alphabay was the biggest Darknet marketplace: with at its peak just over 170.000 active members.

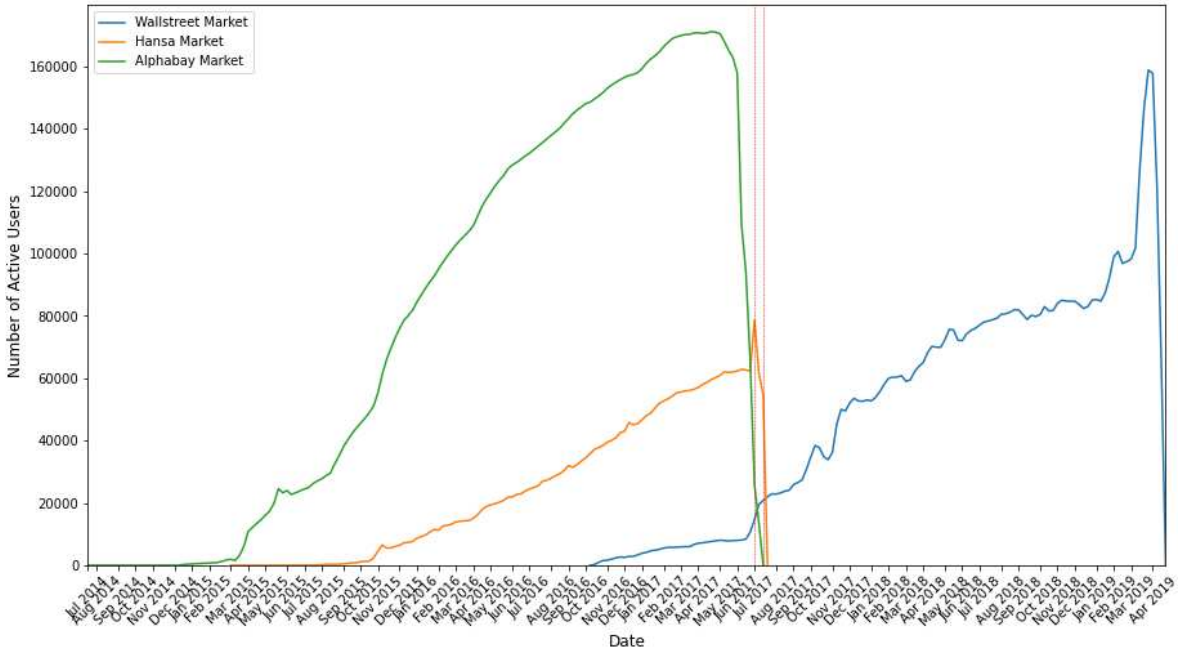


Figure 9.1: Number of Active Users on Darknet Marketplaces

Wallstreet Market is the second biggest, having more than 150.000 active members just before it was shut down. The smallest market of the three is Hansa Market, which had a maximum of 78.000 members. The three shutdown dates can be clearly seen in the image: Alphabay was shutdown on the 4th of July 2017, Hansa Market on the 20th of July 2017 and Wallstreet Market at the end of April 2019. The shutdown dates for Alphabay and Hansa Market are visualised using the two red dotted lines in the figure. Whilst the increase of active users for both Alphabay and Hansa Market is almost gradual, the number of active users for Wallstreet Market fluctuates more. In the few weeks leading up to the shutdown a decrease in the number of active users can be seen for all three marketplaces. This is due to the fact that we use the Last Seen Date as the end date at which a user is active. This decrease can be explained by users not visiting the marketplace daily/weekly and only on moments when they are looking to potentially buy or sell items. Therefore, some active users might have a last seen time a few days or weeks before the takedown date, explaining the already decreasing numbers before the takedown.

Noticeable is also the increase in active members on Hansa Market and Wallstreet Market after the shutdown of their competing biggest market on the darknet. As part of Operation Bayonet (elaborated in Section 2), Alphabay was shut down by the FBI on the 4th of July 2017. This caused a lot of Alphabay's users to migrate to the second biggest marketplace at the time: Hansa Market. This can be seen in the jump of the users of Hansa market around July 2017 in the Figure, however not all

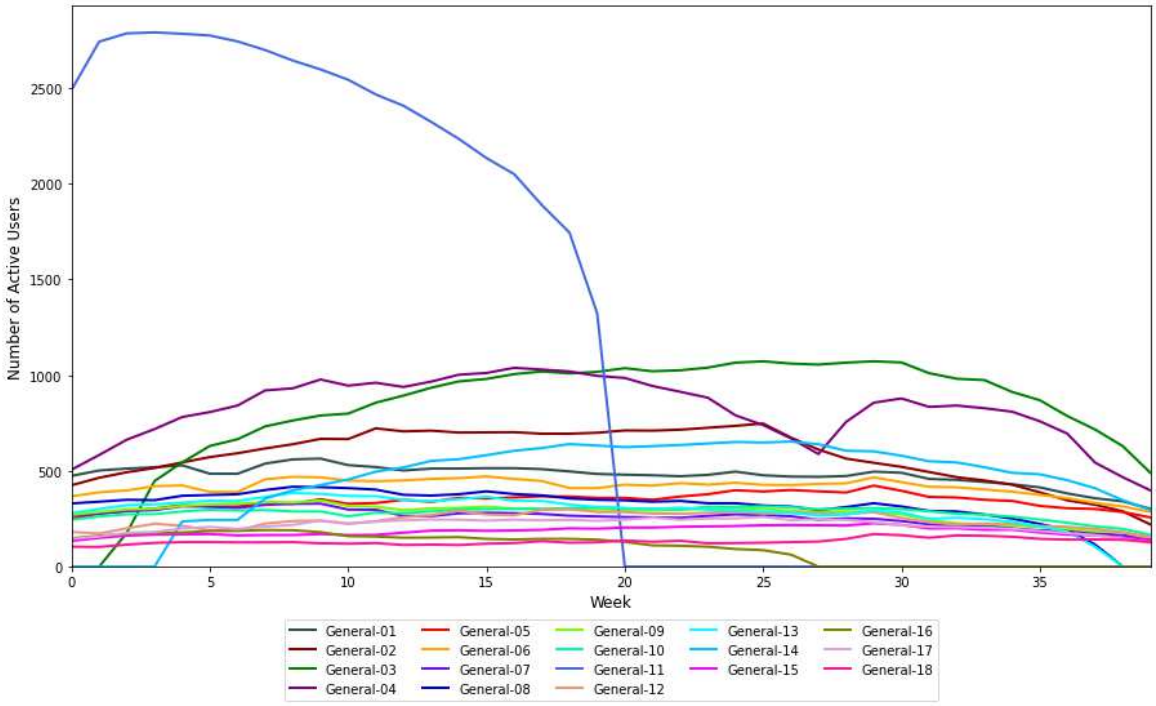


Figure 9.2: Number of Active Users in 'General'-focused Telegram Groups

users migrated from Alphabay to Hansa Market. Shortly after, Hansa Market was also shut down after being run by law enforcement for a number of days.

A similar process happened after Dream Market was shut down in April 2019. Dream Market was the biggest marketplace at the time, with Wallstreet Market being the second biggest. A lot of users migrated to Wallstreet Market after the shutdown of Dream Market, explaining the increase in active users around April 2019. However, similarly to Hansa Market and Alphabay, Wallstreet Market was shut down shortly after.

Telegram Groups

The overview of the average number of users for the Telegram Groups has been split up into 5 different Figures: one for each of the Telegram group focuses. As elaborated on in 5.4.1, the first and last few weeks have been removed from the visualisation to give a more accurate representation.

Figure 9.2 shows a visualisation of the number of active members over the measurement period for all General-focused groups. Figure 9.3 shows the same visualisation as Figure 9.2, only with group 'General-11' removed as to clearly visualise the other

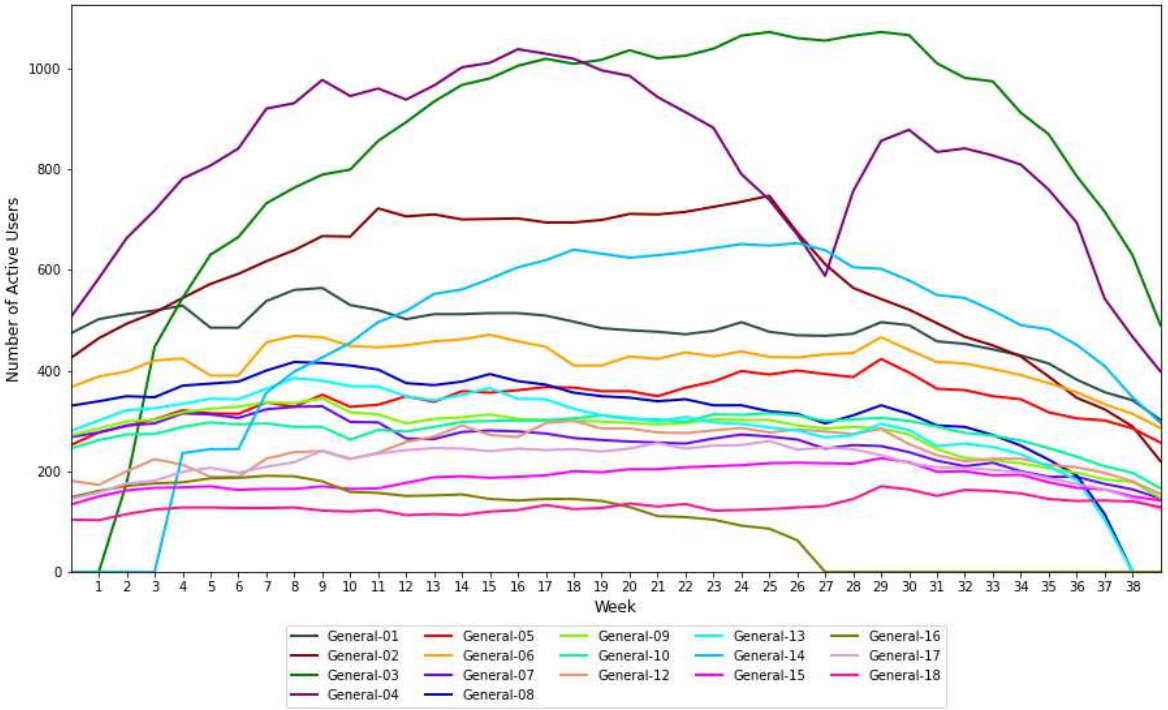


Figure 9.3: Number of Active Users in 'General'-focused Telegram Groups (without General-11)

groups as well. Group General-11 has a much larger number of active users compared to all the other General-focused groups. This is also a group of which there is no more data halfway through the measurement period, as can be seen by the number of active members dropping to zero around week number 20.

Figure 9.3 shows that next to General-11, there are more groups that only have data up to a certain point during the measurement period. This can clearly be seen by the active member numbers of General-10, which reaches zero at week #27. Active user numbers for General-08 and General-16 also decrease to zero at week #38. Active user number for General-13 reach zero just before the end of the measurement period. There can be two reasons for this data not being present: either the group might have been deleted or shut down, or the group stopped being part of the list of groups being scraped for the dataset. In the case of these five groups, only one of them no longer exists: General-16. The other groups do still exist, but their contents are no longer scraped as part of the dataset.

Opposite to groups no longer appearing in the dataset, there are also groups that appear halfway through the dataset. At the start of the measurement period, there is not yet any data on groups General-03 and General-14. Starting from week #1 there is data for General-03, and starting from week #3 there is data for General-14. It is possible that these groups have just been created and set up. However, it is more

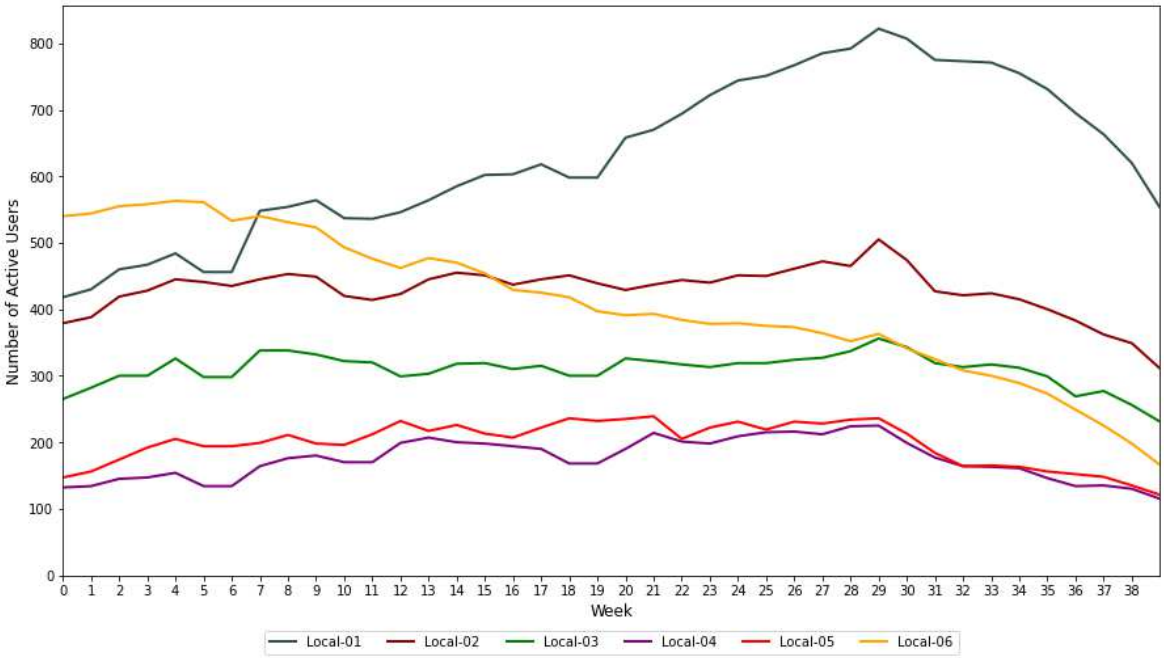


Figure 9.4: Number of Active Users in 'Local'-focused Telegram Groups

likely that these groups only started being part of the list of groups to be scraped for the dataset at that point in time and were already established groups beforehand.

A few interesting points in time can be seen in Figure 9.3. Leading up to week #27, a drop of around 200 users in 4 weeks can be seen in the active user numbers of group General-04. In the following two weeks, the number of active users seems to increase again to a stable number though less big than before. This dive happened around the first weeks of August 2022. In the same weeks, the Dutch Police placed a message in a number of Telegram groups warning (potential) sellers of phishing panels [69]. Looking at the messages in the group around this time confirm that General-04 was one of the groups that this message was sent in.

Figure 9.4 shows a visualisation of the number of active users for all the Local-focused Telegram groups. Most of the groups in this Figure have a steady number of active users that does not change a lot and is typically in the range between 100 and 600 users, with the exception of group Local-1 which grows to 800 users and then suddenly drops to 650 users. Active user numbers in the Local-06 group seem to gradually decline, with the group losing more than 150 active members in the span of 20 weeks. All groups show a drop in the number of active users after week #28, with some groups having a steep increase the week before. Though none of the groups received the message by the Dutch Police, there is a possibility that this increase and following drop in active users is a result of word-of-mouth regarding the

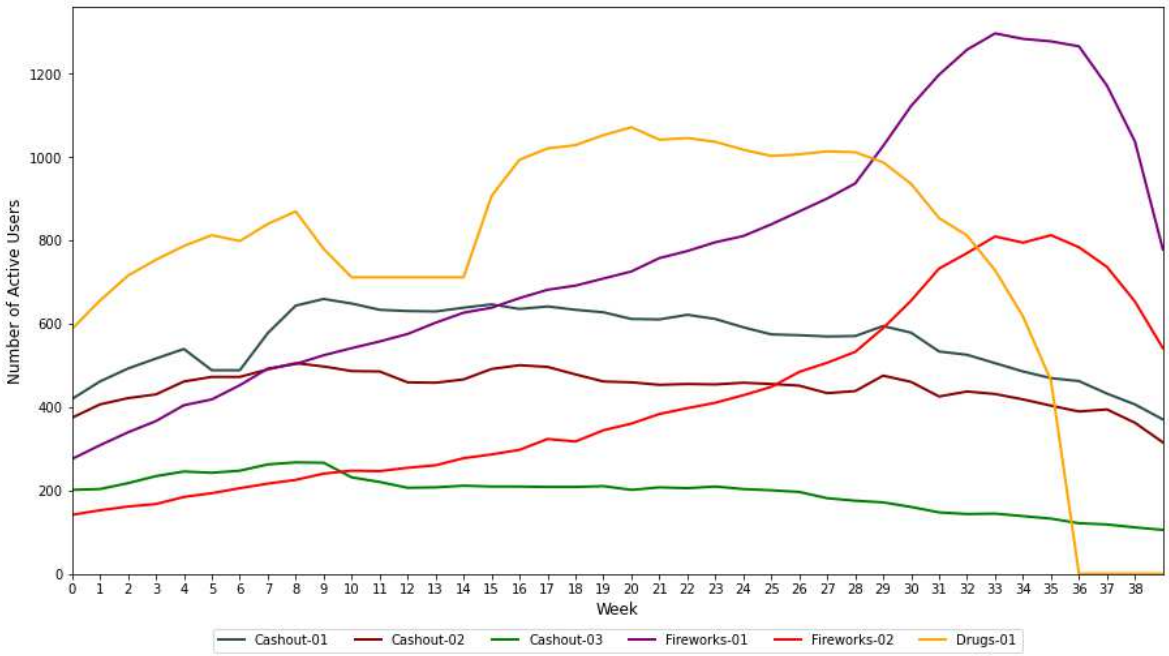


Figure 9.5: Number of Active Users in 'Cashout', 'Fireworks' and 'Drugs'-focused Telegram Groups

message and its contents. Users from affected groups might move to other groups that did not receive a message and are viewed as 'safe', resulting in talk about the message and others leaving the groups.

Figure 9.5 shows the visualisation of the number of active users for all the Cashout-, Fireworks- and Drugs-focused Telegram groups. Between weeks #10 and #14 there is no data for Drugs-01, explaining the lack of increase or decrease in active user numbers. The two Fireworks-focused groups clearly show an increase in active users approaching the end of the year. This can be explained by the fact that leading up new years eve there in an increase in interest for Fireworks. The active user numbers for the Cashout-focused groups remain relatively stable over the measurement period.

9.1.2 Relative Growth

The number of users of the Darknet marketplaces differ a lot from the number of users in the smaller Telegram groups. Therefore we also look at the relative growth of the marketplaces and groups.

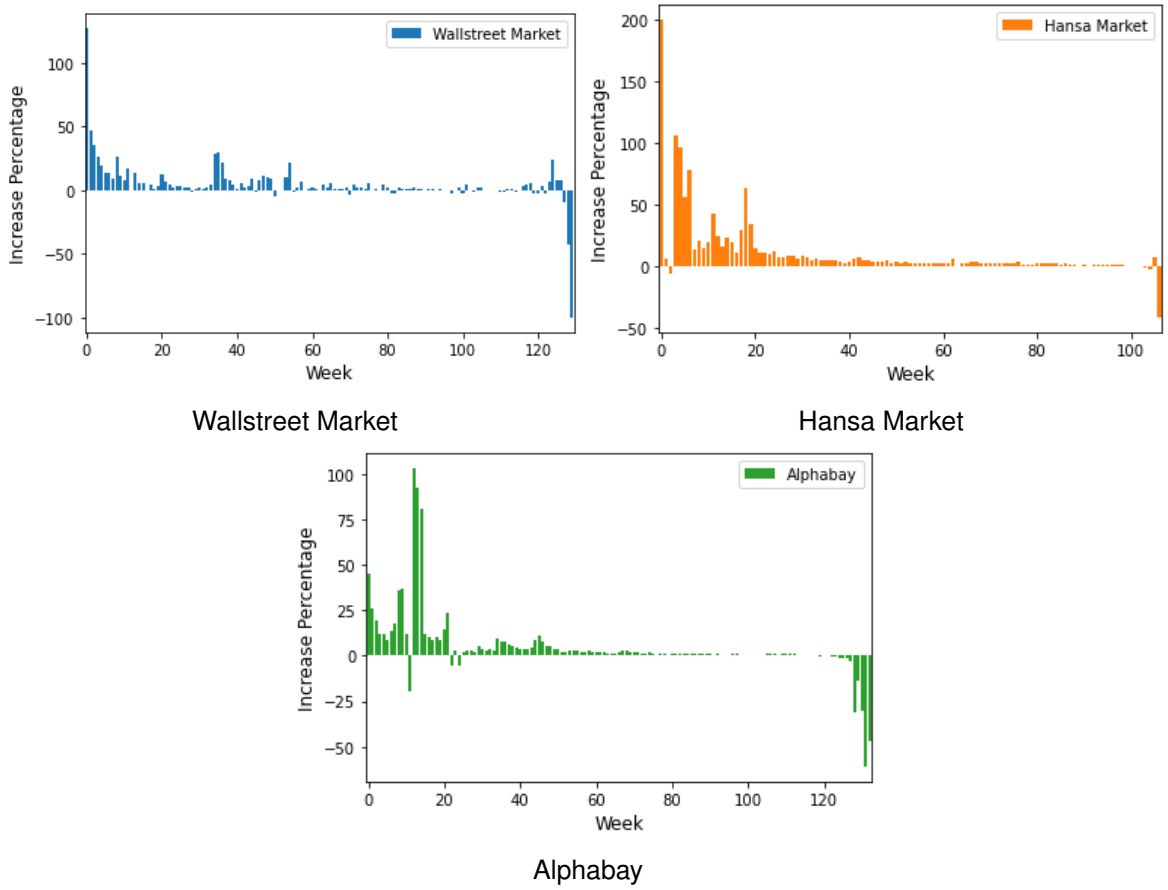


Figure 9.6: Relative Growth of Darknet Marketplaces

Darknet Marketplaces

Figure 9.6 shows the relative growth of active users for each of the three Darknet marketplaces. In the first weeks of all three marketplaces we can see that the percentage with which the active member numbers are increased each week are relatively high compared to the percentages later in time. This is because the marketplaces have just started and therefore do not yet have a large user base, leading to a higher increase percentage relative to the total number of active users. The same applies for the final weeks, after which the marketplaces are shut down and therefore show a massive decrease in active members each week. Interesting to note is that in Figure 9.6b the increase in users after the shutdown of Alphabay can clearly be seen in the relative growth percentage of Hansa Market around week #110.

Figure 9.7 shows the same relative growth percentages for the three Darknet marketplaces as Figure 9.6 without the first and last 15 weeks of data. This Figure gives us a better overview of the growth of the marketplaces during their normal operation

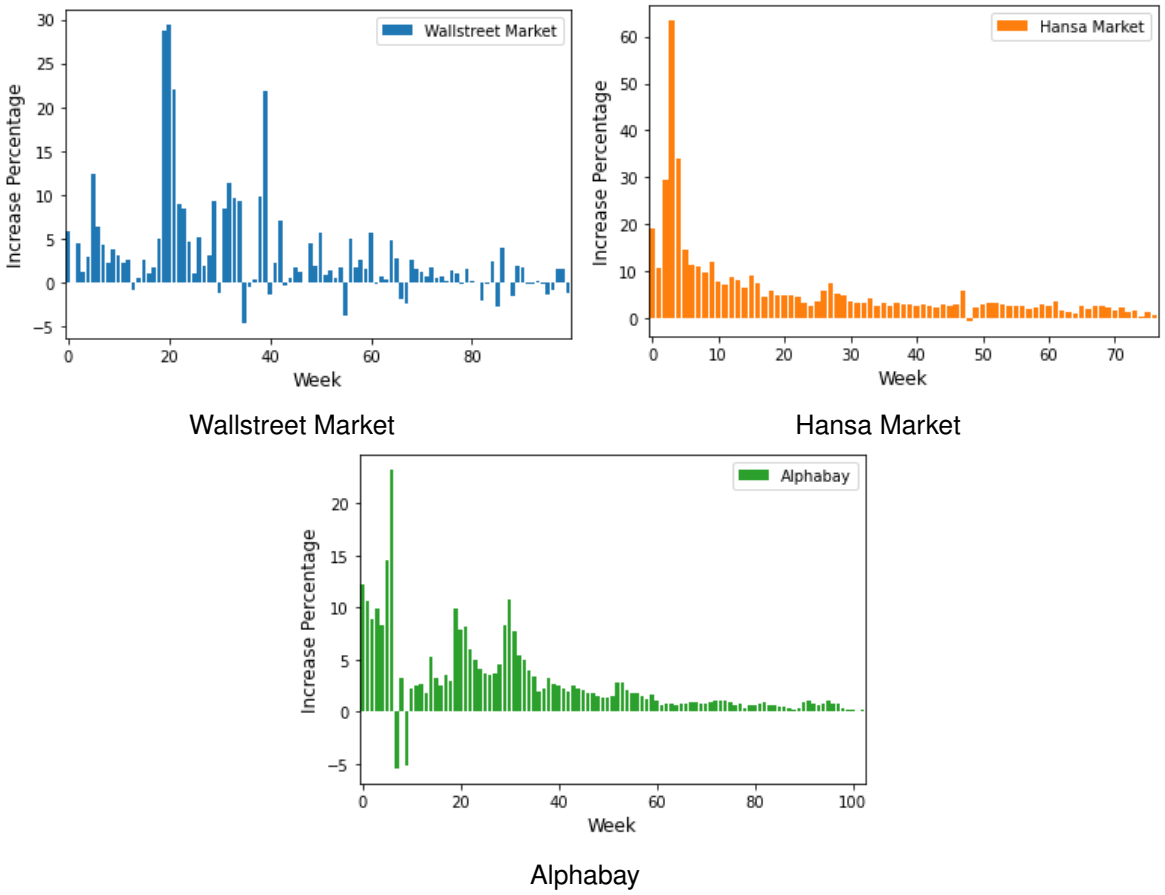


Figure 9.7: Relative Growth of Darknet Marketplaces without first and last 15 weeks
Note: all graphs have a different y-axis scale

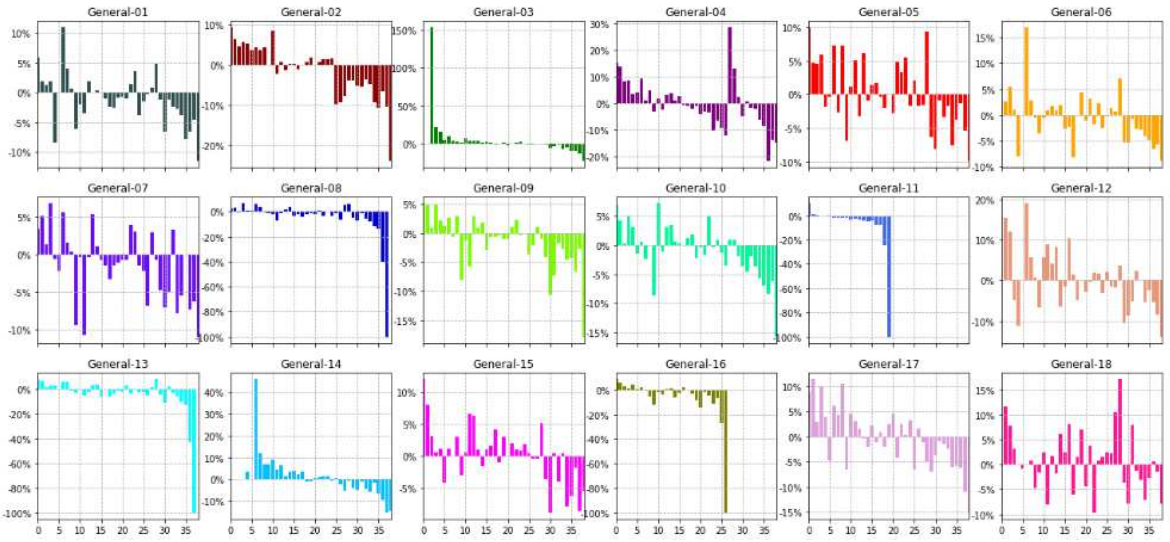


Figure 9.8: Relative Growth of 'General'-focused Telegram Groups
Note: all graphs have a different y-axis scale

after gathering an initial user base and before their shutdown.

We can see that the user base of Wallstreet Market is more volatile than those of Hansa Market and Alphabay. There are a number of weeks where there is a negative relative growth on Wallstreet Market, meaning that the active user base is actually shrinking. However, the majority of the weeks the relative growth is positive and therefore the market is still growing over time.

Both Hansa Market and Alphabay seem less volatile, having only one or two weeks where the relative growth is negative. What is notable is that for both marketplaces the relative growth percentage in terms of the total number of active users gradually decreases as time goes on. This means that both marketplaces are steadily growing at a close to linear rate, as confirmed by Figure 9.1.

Telegram Groups

Figure 9.8 shows the relative growth per week for each of the 'General'-focused Telegram Groups. Similarly to the results in Section 9.1.1 the first and last weeks have been removed from the visualisation. What can be seen from all sub figures is that the relative growth for most of the groups is very volatile. Groups such as General-05 and General-18 give a great example of this, as one week the group is growing by 6%, whilst the next week the group is shrinking by 7%. These groups are the groups that remain at a steady number of total active users over time, as can be

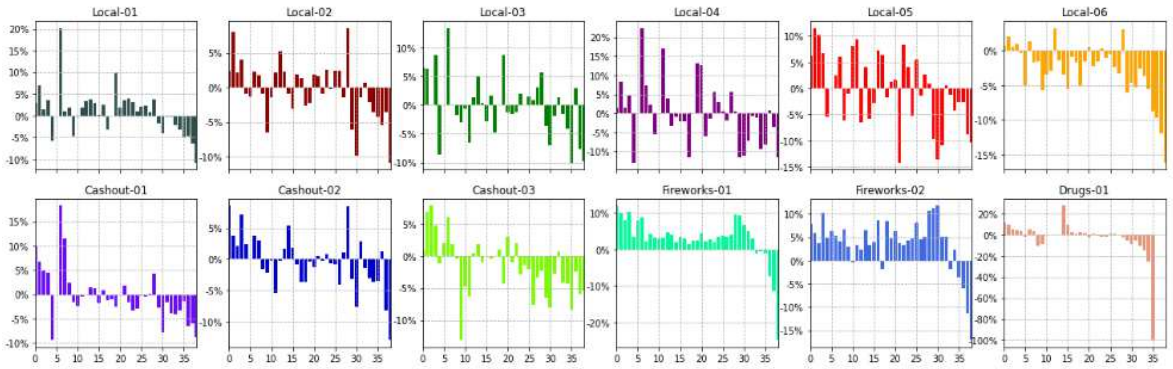


Figure 9.9: Relative Growth of 'Local'-, 'Cashout'-, 'Fireworks'- and 'Drugs'-focused Telegram Groups
Note: all graphs have a different y-axis scale

seen in Figure 9.3.

The groups that we do not have any more data on halfway through the measurement period, either due to the group no longer being part of the measurements or because the group shut down clearly show the negative growth in the last weeks of measurement. This can be seen in the graphs for General-08, General-10, General-11 and General-16.

Figure 9.9 shows the relative growth percentage for all 'Local'-, 'Cashout'-, 'Fireworks'- and 'Drugs'-focused Telegram Groups. From the figure we can see that most Local-focused groups switch between an increase one week and a decrease the next week, indicating no increasing or decreasing member numbers trends.

Whilst the patterns in the relative growth graphs of most groups look similar, the two Fireworks-focused groups show a different shape. The relative growth remains positive up until almost the end of the measurement period, and in the case of Fireworks-02 even increases leading up to the end. This can be explained by the increased interest in Fireworks nearing New Year's Eve. However, this does show that when compared to the pattern of relative growth of other groups, Fireworks-focused groups are clearly an outlier that do not adhere to the established pattern.

Comparison

When we compare the visualisations on the Darknet marketplaces in Figure 9.7 to those of the Telegram groups in Figures 9.8 and 9.9 we see that the relative growth graph of Wallstreet Market is the most similar to the Telegram groups compared

to the other two Darknet marketplaces. This as the relative growth for Wallstreet Market also has negative percentages, which is also the case for most of the Telegram groups. Darknet marketplaces seem to steadily grow, whilst most Telegram Groups hover around a group-specific number of active users and do not see any big growth or decline. The only exception to this observation are the Fireworks-focused Telegram Groups which appear to mimic the steady growth of the Darknet marketplaces. However, as the measurement period for the Telegram groups ended just before new year's eve there is a strong suspicion that this growth would not continue into the new year. This due to the fact that there is an increased demand for and attention on Fireworks specifically at the end of the year.

9.1.3 New and Leaving Users

A small increase in the number of active users can be caused by a small number of users leaving and a slightly larger number of new users joining. However, it can also be caused by a large number of users leaving and an even larger number of new users joining. Therefore the relative growth does not say anything about churn, and the trends in the newly joining users and leaving users.

Darknet Marketplaces

Figure 9.10 shows the percentage of new users and leaving users per week for each of the three Darknet Marketplaces. When we look at the outlier in both new users and leaving users around week #7 of Alphabay we see that whilst the actual growth is relatively small, the number of users expanded by more than 60% with new users. Similarly, almost 40% of existing active users left. A similar situation occurs at the peak around week 40 in Figure 9.7a. Here we see that the number of users increases by more than 20% that week. However, when looking at the same week in Figure 9.10a we see that the percentage of new users is relatively small. What makes it that the percentage increase of users is so big for this week is the fact that the percentage of users leaving is small.

When looking at the overall trends we see that for all three marketplaces the percentage of new and leaving users stays relatively the same and equal for all three marketplaces. The percentage of new users stays around 18% each week for all three marketplaces. Similarly, the percentage of leaving users is on average around 15% for all three marketplaces.

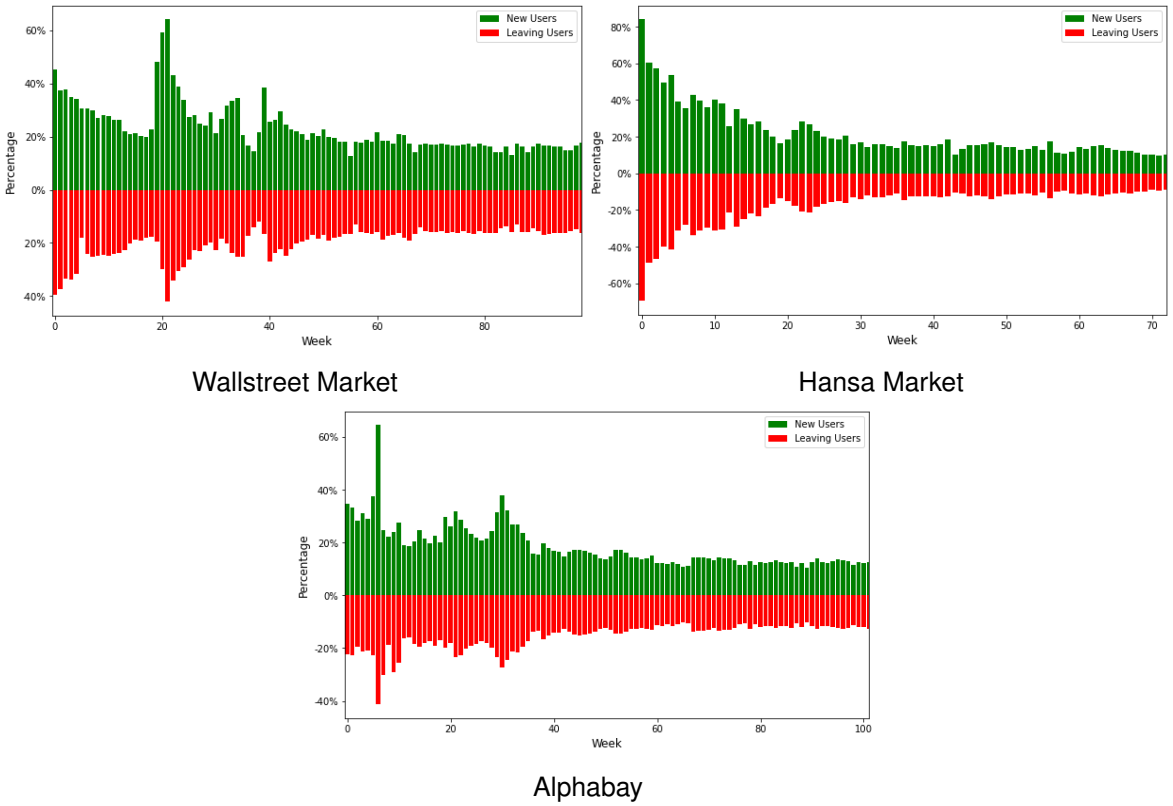


Figure 9.10: Percentage of new users and leaving users for Darknet Marketplaces
Note: all graphs have a different y-axis scale

Telegram Groups

Figure 9.11 shows the percentage of new and leaving users with regards to the total number of users for all 'General'-focused Telegram groups. We can clearly see the high percentage of leaving users for four groups that stop halfway through our measurement data: General-08, General-11, General-13 and General-16. In the case of group General-10 it is less obvious, as until the final weeks there is still an increase of 20% new users in the final week of data. When we compare the data in this figure with Figure 9.8 and look at General-09, we see that this group has negative growth for more than half of the time. However, when we look at the visualisation of the new and leaving users we can see that in the majority of the time this group gets an increase of more than 10% new members. The reason why the growth is so small is because the percentage of leaving users is relatively big.

Figure 9.12 displays the percentage of new and leaving users for the 'Local'-, 'Cashout'-, 'Fireworks'- and 'Drugs'-focused Telegram Groups. Again we can see the increase in new users towards the end of the measurement period in both Fireworks-01 and Firework-02.

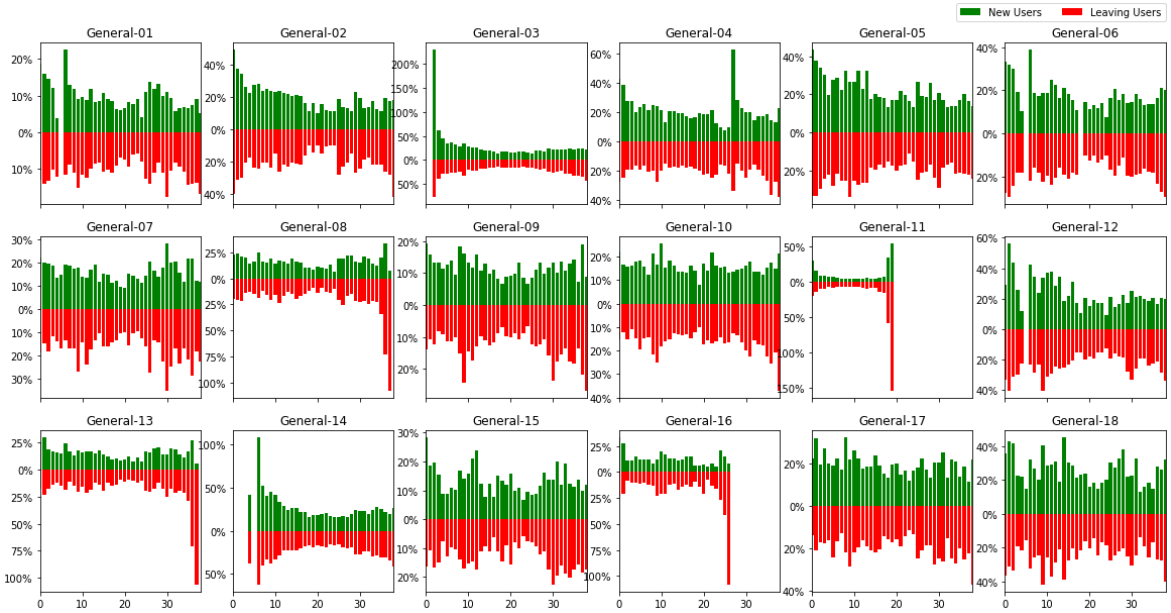


Figure 9.11: Percentage of new and leaving users for 'General'-focused Telegram Groups
Note: all graphs have a different y-axis scale

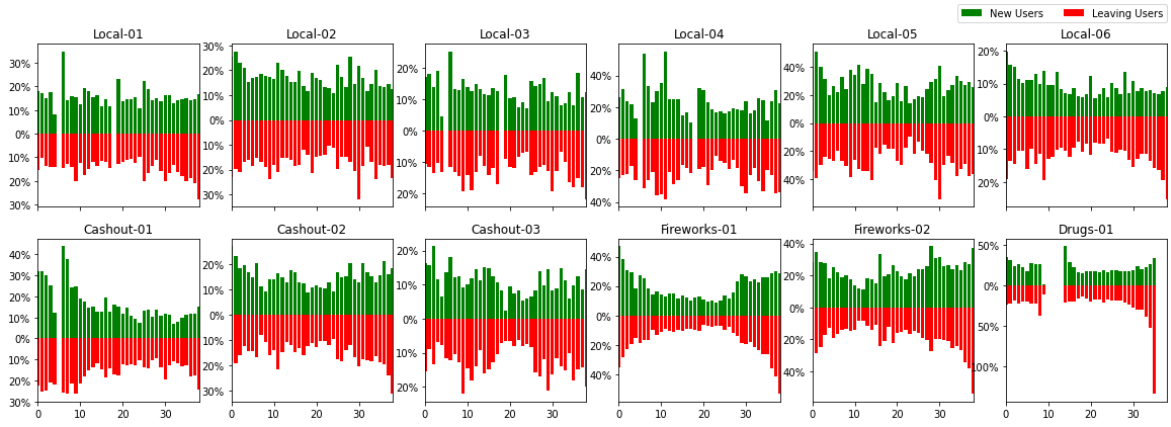


Figure 9.12: Percentage of new and leaving users for 'Local'-, 'Cashout'-, 'Fireworks'- and 'Drugs'-focused Telegram Groups
Note: all graphs have a different y-axis scale

	Average Percentage of New Users	Average Percentage of Leaving Users
Wallstreet Market	23,18%	20,03%
Hansa Market	21,89%	17,87%
Alphabay	18,49%	15,69%
Combined	21,19%	17,86%

Table 9.1: Average percentage of new and leaving users for Darknet Marketplaces combined

	Average Percentage of New Users	Average Percentage of Leaving Users
General	17,51%	18,57%
Local	17,46%	17,96%
Cashout	14,17%	14,87%
Fireworks	21,22%	18,43%
Drugs	18,27%	21,12%
Combined	17,47%	18,15%

Table 9.2: Average percentage of new and leaving users for all Telegram Groups combined

Comparison

Table 9.1 shows the average percentages of new users and leaving users for the Darknet Marketplaces, as well as a combined average for all Darknet marketplaces. Similar values for the Telegram groups can be found in Table 9.2. From these tables and the figures we see that in general, the percentage of new users for Darknet marketplaces is higher than for Telegram groups. The average percentage of leaving users is also smaller for the Darknet marketplaces than of Telegram groups. Similarly to the observation in 9.1.2, we can again see that the two Fireworks groups follow a similar pattern as that of the Darknet marketplaces. As can be seen in the figures, the Telegram groups are much more dynamic and their member numbers fluctuate more than those of the Darknet marketplaces. A possible reason for this could be that it is a lot easier to setup a Telegram group than it is to set up an entire marketplace on the Darknet. This leads to there being a lot more Telegram groups where users can get the same things, allowing them much more freedom in choosing which groups to be active in.

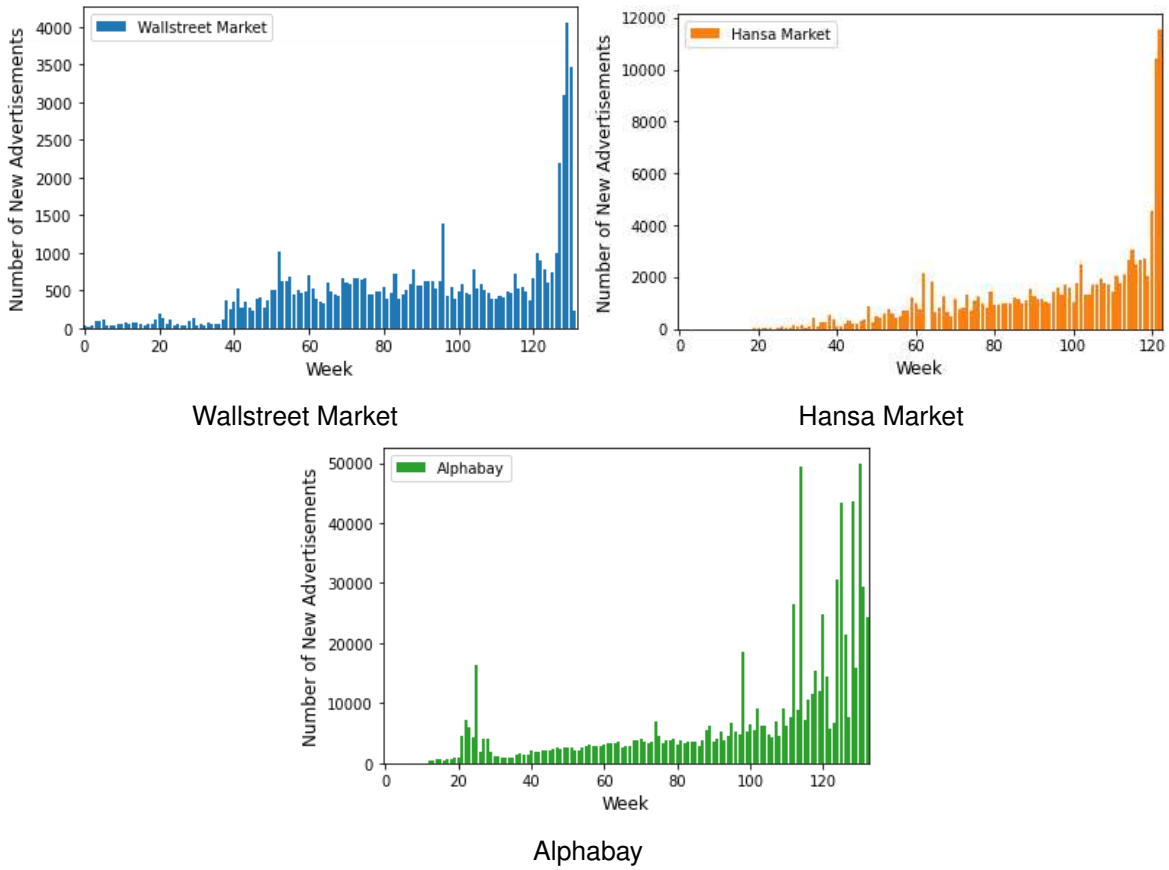


Figure 9.13: Number of new Advertisements per Week for Darknet Marketplaces
Note: all graphs have a different y-axis scale

9.2 Advertisements over Time

Darknet Marketplaces

Figure 9.13 shows the number of new advertisements per week for the three Darknet marketplaces. As there are differences in size for the three marketplaces, the number of new advertisements per week differs as well. On average, each week 483 new advertisements are placed on Wallstreet Market. Similarly, for Hansa Market and Alphabay this is around 1.001 and 6.223 new advertisements per week respectively. We see that for all three marketplaces, the number of new advertisements per week steadily increases. Figure 9.13b also clearly shows the massive increase in the number of new advertisements in the final two weeks of Hansa Market's operation. These are the two weeks just after the takedown of Alphabay, when a lot of users moved to Hansa. A similar jump can be seen in Figure 9.13a around week 40. This jump is at the point in time where both Hansa Market and Alphabay Market were shut down, as can be seen in Figure 9.1. Overall, the trend can be seen that

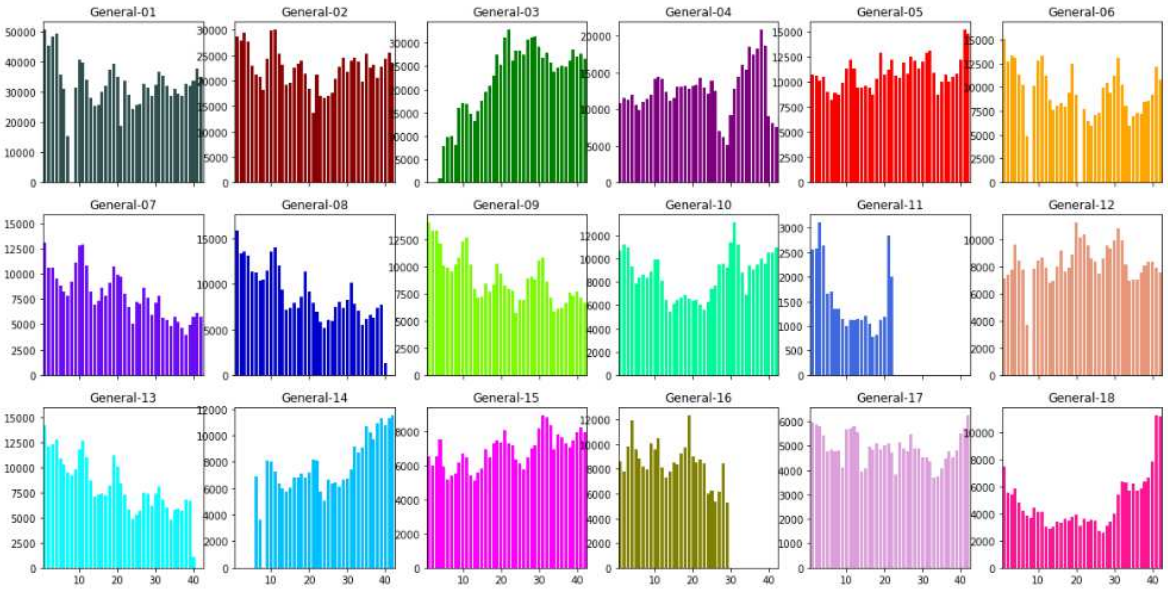


Figure 9.14: Number of advertisements per week for General-focused Telegram Groups
Note: all graphs have a different y-axis scale

the number of advertisements steadily increases with the number of active users. When we look at the number of new advertisements for Alphabay in Figure 9.13c we can see a few outliers where the number of new advertisements per week is higher than 40.000. In these cases a large number of credit card login details were posted on the marketplace. However, instead of all these details being sold as part of one package listing, which is usually the case, the login details for each single credit card were listed as a separate item, explaining the large number of new advertisements.

Telegram Groups

Figure 9.14 shows the number of advertisements per week for each of the General-focused Telegram Groups. This Figure shows that groups General-01 and General-02 get the largest number of advertisements per week. There are weeks where 50.000 advertisements are sent in group General-01. Similarly, this number is close to 30.000 for group General-02. The group in which on average the least advertisements are sent per week is group General-11, though at minimum more than 700 advertisements were sent each week in this group. The mean number of advertisements sent each week in General-focused groups is 9.982.

Figure 9.15 shows the number of advertisements per week for each of the Local-

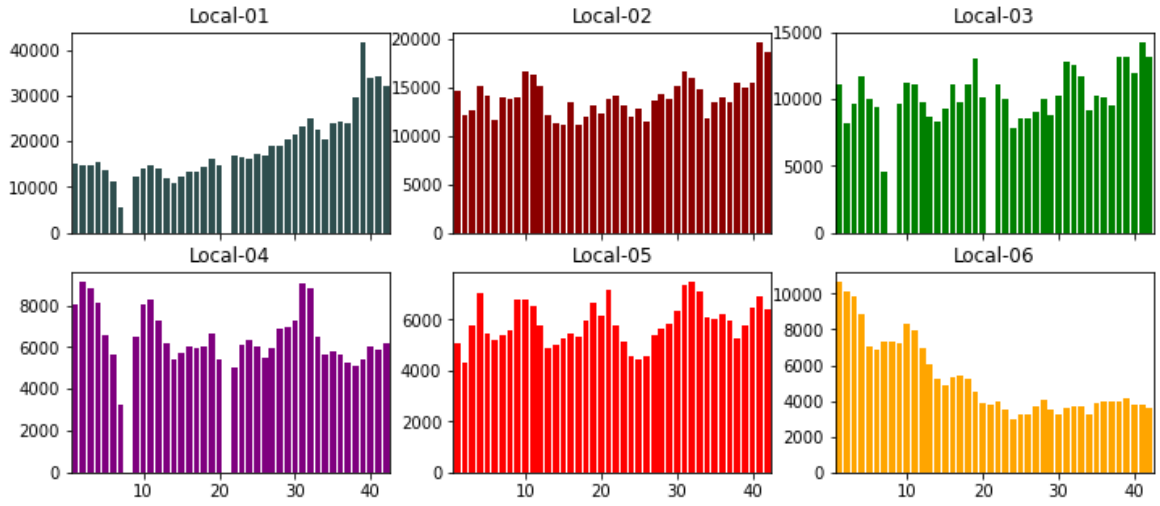


Figure 9.15: Number of advertisements per week for Local-focused Telegram Groups
Note: all graphs have a different y-axis scale

focused groups. A steady increase in the number of advertisements can be seen for group Local-01. Similarly, a steady decrease can be seen for group Local-06. The group Local-05 contains the least number of advertisements per week on average compared to the other Local-focused groups. On average, 9.361 advertisements are sent each week in Local-focused groups.

The number of advertisements per week for each of the Cashout-, Fireworks- and Drugs-focused groups can be found in Figure 9.16. A steady increase of the number of advertisements in the final 15 weeks can be seen for both Fireworks-focused groups. A decrease in the number of advertisements per week can be seen for group Cashout-03. On average, Cashout-focused groups contain 9.621 advertisements per week. Fireworks-focused groups contain 5.401 advertisements on average per week, whilst the Drugs-focused group contains 7.722 advertisements on average per week.

Comparison

When we compare the advertisement numbers each week for the Darknet marketplaces to those of the Telegram Groups it is evident that there are a lot more advertisements posted in the Telegram Groups compared to the Darknet marketplaces. Important to note is that whilst a listing/advertisement can only be placed once on the Darknet marketplaces, users in Telegram groups have the opportunity to promote their advertisement as many times as they would like. Therefore, the actual

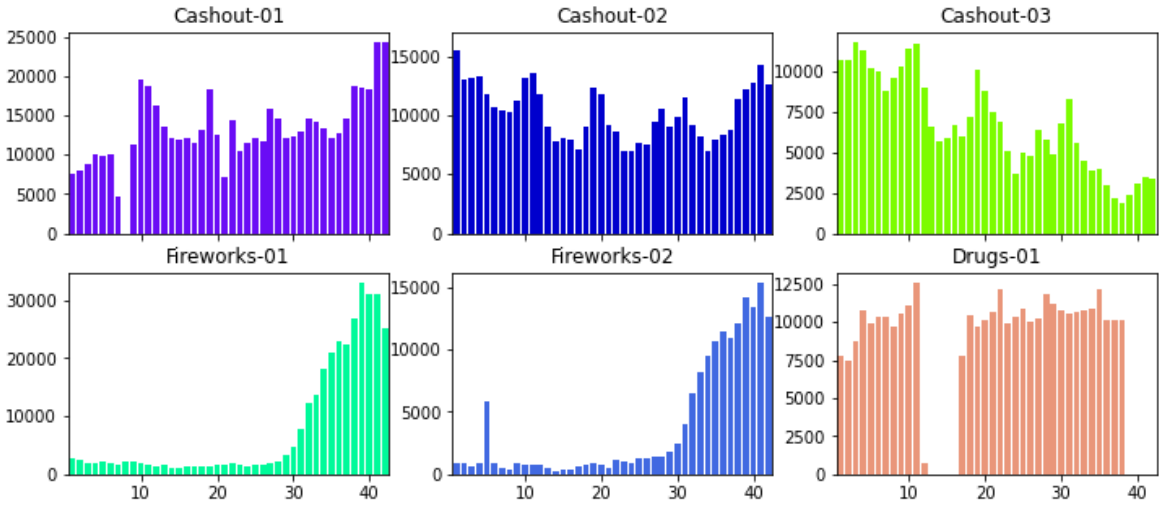


Figure 9.16: Number of advertisements per week for Cashout-, Fireworks- and Drugs-focused Telegram Groups
Note: all graphs have a different y-axis scale

number of unique advertisements in the Telegram groups each week is expected to be much lower than the numbers shown in Figures 9.13a, 9.13b and 9.13c.

The number of advertisements per week for the Darknet marketplaces show a steady increase (disregarding the final few weeks of operation of all three marketplaces). However, there are only a few Telegram groups that show a similar steady increase in the number of advertisements per week. Most Telegram groups have a steady number of advertisements that does not show any significant increase or decrease. A few groups show a specific decrease in the number of advertisements. The Fireworks-focused groups match the most to the shape of the Darknet Marketplaces, though their average advertisement numbers per week are higher.

Chapter 10

Conclusion

This chapter wraps up our research by answering the research questions and listing our contributions to the field.

SQ1: What are the differences in organisational structure between traditional criminal marketplaces and emerging digital criminal marketplaces on Telegram?

A big similarity between the traditional criminal marketplaces and the newly emerging digital marketplaces on Telegram is the amount of administrators and staff running the marketplaces. Even though the marketplaces on the Darknet are at minimum 50 times bigger than the marketplaces on Telegram in terms of users, this major difference in user numbers does not appear to equate to a larger number of administrative staff running the marketplaces. Therefore, there appears to be a sweet spot number of administrators needed to keep a criminal marketplace running; around 3 to 4 administrators. However, administrative users in the Telegram marketplaces can also be bots instead of human users, which is not the case for the Darknet marketplaces. These bots are generally used for simple, repetitive tasks such as monitoring spam and enforcing messaging rules. On the Darknet marketplaces these tasks are not performed by actual administrative staff, but are part of the marketplace mechanism not needing user action. Therefore, if we look at human administrators there are slightly more administrators needed to run Darknet marketplaces. However, as these marketplaces are much bigger, the number of administrators per user is a lot smaller for Darknet marketplaces compared to the Telegram marketplaces. Therefore we conclude that the Telegram marketplaces are much more work-intensive in terms of the number of administrators needed to run

the marketplace.

Where the Darknet marketplaces use feedback systems and disputes to streamline the ordering process and improve the user experience on the marketplace, these systems are not in place for the Telegram marketplaces. One major difference is that the entire ordering process is handled by the Darknet marketplaces, but the Telegram marketplaces are mainly used as an advertisement channel where the actual ordering is done through private messages with the vendors directly. The feedback systems of the Darknet marketplaces and disputes are used to help the buyer in their ordering process and provide extra information and more security when ordering. In the case of the Darknet marketplaces buyers can make a more informed decision on who to order from based on the feedback ratings the vendor has gotten in the past. Similarly, in the case something is wrong with an order users have the option to open a dispute and possibly get their money back based on the ruling of the marketplace. As Telegram marketplaces do not have theses systems in place, users buying goods through these marketplaces have a higher risk of getting scammed and losing their money due to the lack of structured ordering systems.

As there is no generalised ordering system, there are also no specified mandatory payment methods for orders in the Telegram groups. Orders are only allowed to be paid through cryptocurrency on the Darknet marketplaces, which is difficult to trace back to the person behind the payment. As no such rule is in place in the Telegram groups, buyers can pay for their orders with a number of different methods next to cryptocurrency. Though this gives users more options, payment with most of these options can also be easily traced back to the user, making it lot less secure when buying illegal goods.

SQ2: How do users engage with the different types of marketplaces

In general, the Telegram marketplaces are much smaller than the Darknet marketplaces in terms of the total number of users. However, the percentage of active users is double that of the Darknet marketplaces on the Telegram marketplaces. This suggests that the users on the Telegram marketplaces engage in a different way than the users on the Darknet marketplaces. The probable reason for this is twofold: the way the Telegram marketplace is set up allows for much more user activity and the Telegram marketplaces are easier to access than the Darknet marketplaces. The Telegram marketplaces allow for more user activity in the sense that these marketplaces are one big messaging group where all users can send messages and reply on each other, similar to a forum. This is not the case for the Darknet marketplaces,

which do not allow users to comment on specific advertisements and purely operate as a marketplace instead of a messaging forum. Next to this a certain level of technical skill is needed to access marketplaces on the Darknet, using special software such as a Tor browser and knowing the specific URL that hosts the marketplace. This required level of skill is much lower when using Telegram, as it is an app that can be installed through an app store on almost any mobile phone. Users can find the marketplaces by using the search function built into the Telegram app. This difference in technical skill level needed to access both marketplace may mean that the more technologically skilled users use the Darknet marketplaces, while the less technologically skilled users tend to use the Telegram marketplaces.

A much larger portion of the userbase of the Telegram marketplaces are vendors compared to that of the Darknet marketplaces. These vendors on the Telegram marketplaces also have a much larger number of different listings compared to the vendors on the Darknet marketplaces. Therefore, while the Darknet marketplaces are bigger in terms of total users, the Telegram marketplaces are bigger in terms of more vendors and more unique listings. Which leads to the assumption that Telegram marketplaces are more attractive to vendors (with both good and bad intentions) than Darknet marketplaces.

SQ3: What are the differences in types of goods and services being advertised on traditional criminal marketplaces and emerging digital criminal marketplaces on Telegram?

There are a few notable differences in the types of goods and services being advertised on the two types of marketplaces. Firstly, Fireworks are much more advertised on the Telegram marketplaces than on the Darknet marketplaces. We believe this to be due to a few different reasons. Only in the recent few years has the sale of illegal Fireworks increased in the Netherlands due to the restrictions on Fireworks becoming more strict and cities banning Fireworks all together. As Fireworks become less easily available, there is a natural progression to the sale of these products through Telegram (and other) marketplaces. However, as the advertisements on the Darknet marketplaces are from before this increase in restrictions, we cannot definitively say that there would not have been an increase of Fireworks advertisements on the Darknet marketplaces as well.

Secondly, there are a lot more Cashout advertisements on the Telegram marketplaces. We believe this to be due to these Telegram marketplaces being used to find money mules to launder money. In such a case an advertisement is placed ask-

ing for access to a bank account and/or debit card which is in turn used to deposit and withdraw funds in exchange for a percentage of the total funds. Such operations and advertisements are not present on the Darknet marketplaces, as the Darknet marketplaces only allow advertisement offers and no advertisement requests.

Overall, the Darknet marketplaces are mostly focused on the sale of Drugs and Pharmaceuticals. In terms of the distribution of the types of goods and services being advertised, all Darknet marketplaces look similar. This is not the case for the different Telegram marketplaces. The types of goods and services advertised can vary a lot between the different Telegram marketplaces, depending on where the users of the Telegram marketplace originate from and what the original aim of the administrators of the marketplaces was. Therefore the Darknet marketplaces have a more generalised distribution of the different types of goods and services, whilst some Telegram groups have a more distinct speciality with regards to the goods and services advertised.

SQ4: How is the usage of both traditional criminal marketplaces and emerging digital criminal marketplaces on Telegram developing over time?

A major observation on the development of the different types of marketplaces over time is that the Darknet marketplaces are steadily growing over time in terms of users. The Telegram marketplaces however, have a set number of users that does not seem to steadily increase. The member numbers of the Telegram groups fluctuate much more than those of the Darknet marketplaces. Where the data rarely shows the Darknet marketplace shrinking in terms of the total number of active users, with the exception of the final weeks before the shutdown, this is a regular occurrence for the Telegram marketplaces. The member numbers of the Telegram groups seem to correlate to real world events in the Netherlands, such as the increased demand for Fireworks just before New Year's Eve. This is not the case for the Darknet marketplaces.

More advertisements are placed per week on the Telegram marketplaces than on the Darknet marketplaces. The Telegram marketplaces allow users to post their advertisements multiple times, which is not the case for the Darknet marketplaces. What can be seen in both types of marketplaces is that as the number of users increases, the number of advertisements increases as well.

MRQ: What are the difference and similarities between traditional digital criminal marketplaces and emerging criminal marketplaces on Telegram?

Using the answers to the four subquestions, we determine that the Telegram marketplaces are more focused on the initial ease of use of the advertisements in the marketplace itself. The marketplace can be accessed by simply installing the Telegram app, which can be installed on almost every (modern) mobile phone, the specific marketplaces can then be found using the built-in search function of the Telegram app. There are a number of different marketplace groups with either a very specific focus on a service or product, or a more general focus where a number of different types of products and services are advertised. Most messages are written in the native language of the users using the marketplace, the goods and services are shipped from the country of origin of the marketplace and there are a large number of possible payment options. However, the marketplaces are purely there as advertisement boards. As soon as users want to purchase goods or service advertised they need to contact the seller directly and the entire purchasing process is done outside of the marketplace.

Marketplaces on the Darknet are more difficult to access by requiring more technical knowledge to access the Darknet and the specific marketplace URL. These marketplaces also have a more general focus where a very large category of different goods and services are advertised to users worldwide. However, the entire ordering process can be done on the marketplace and the marketplaces have a lot more systems in place to protect both the buyer and the seller. Next to this, payment is also only available using cryptocurrencies to limit the ability to trace a purchase back to an individual.

In conclusion, Telegram marketplaces are in general easier to use. However, for this ease of use users compromise by not having access to systems that can protect both buyer and seller in the ordering process, which Darknet marketplaces do have.

10.1 Discussion & Future Work

The results of this research bring up new questions with regards to the evolution of criminal marketplaces on the Darknet and Telegram. The current research has evaluated the differences between the Darknet marketplaces that operated between 2014 and 2019 and the Telegram marketplaces in operation in 2022. As these timelines do not overlap and one time period is much longer than the other, the con-

clusions could be different should all data be from the same time period. Next to this there is no data from the initial start and the eventual shutdown of the Telegram Marketplaces, which is present for the Darknet Marketplaces. Therefore further research on the differences between the two types of marketplaces during the same time period can give valuable insight in the current trends on digital criminal marketplaces.

As described in Chapter 9, Fireworks-focused groups are most similar to the Darknet marketplaces. However, as suggested we believe this to be due to the increase in demand for Fireworks nearing New Year's Eve. As there was no data from after New Year's Eve, having this data might give valuable insight in if these groups are actually similar or if our beliefs were correct.

Bibliography

[1] V. Adewopo, B. Gonen, S. Varlioglu, and M. Ozer, “Plunge into the underworld: A survey on emergence of darknet,” in *2019 International Conference on Computational Science and Computational Intelligence (CSCI)*, Dec. 2019, pp. 155–159.

[2] Kaspersky, “What is the deep and dark web?” https://www.kaspersky.com/resource-center/threats/deep-web, Aug. 2021, accessed: 2022-4-19.

[3] A. Greenberg, “Hacker lexicon: What is the dark web?” *Wired*, Nov. 2014.

[4] A. Demchenko, “The difference between surface web, dark web, and deep web,” https://data-ox.com/web-dark-web-and-deep-web/, Jan. 2021, accessed: 2022-4-19.

[5] TOR, “The tor project,” https://www.torproject.org/, accessed: 2022-4-19.

[6] D. Goldschlag, M. Reed, and P. Syverson, “Onion routing,” *Commun. ACM*, vol. 42, no. 2, pp. 39–41, Feb. 1999.

[7] A. K. Jadoon, W. Iqbal, M. F. Amjad, H. Afzal, and Y. A. Bangash, “Forensic analysis of tor browser: A case study for privacy and anonymity on the web,” *Forensic Sci. Int.*, vol. 299, pp. 59–73, Jun. 2019.

[8] B. Conrad and F. Shirazi, “A survey on tor and I2P,” http://i2p2.de/_static/pdf/icimp_2014_1_40_30015.pdf, accessed: 2022-4-25.

[9] B. Zantout, R. Haraty, and Others, “I2P data communication system,” in *Proceedings of ICN*. Citeseer, 2011, pp. 401–409.

[10] R. Graham and B. Pitman, “Freedom in the wilderness: A study of a darknet space,” *Convergence*, vol. 26, no. 3, pp. 593–619, Jun. 2020.

[11] I. Clarke, O. Sandberg, M. Toseland, and V. Verendel, “Private communication through a network of trusted connections: The dark freenet,” *Network*, 2010.

[12] G. P. Paoli, J. Aldridge, N. Ryan, and R. Warnes, “Behind the curtain: The illicit trade of firearms, explosives and ammunition on the dark web,” Jul. 2017.

[13] A. Afilipoaie and P. Shortis, “The growing industry of darknet marketing,” https://www.swansea.ac.uk/media/The-Growing-Industry-of-Darknet-Marketing.pdf, 2015, accessed: 2022-11-10.

[14] P. Goonetilleke, A. Knorre, and A. Kuriksha, “Hydra: Lessons from the world’s largest darknet market,” Jun. 2022.

[15] P. Shortis, “GDPO situation analysis, june : From dealer to doorstep – how drugs are sold on the dark net,” https://www.swansea.ac.uk/media/From-Dealer-to-Doorstep-How-Drugs-Are-Sold-On-the-Dark-Net.pdf, Jun. 2015, accessed: 2022-11-10.

[16] A. Evangelista, “Darknet markets, competitive strategies in the underground of illicit goods,” 2018.

[17] Bitpanda, “What are multi-signature wallets and how do they work?” https://www.bitpanda.com/academy/en/lessons/what-are-multi-signature-wallets-and-how-do-they-work/, May 2022, accessed: 2022-10-19.

[18] M. Barbaś, “Instability in english language darknet, is hydra about to take over?” https://nethone.com/post/instability-in-english-language-darknet-hydra-darknet-marketplace, accessed: 2022-11-10.

[19] M.-H. Maras, “Inside darknet: the takedown of silk road,” *Crim. Justice Matters*, vol. 98, no. 1, pp. 22–23, Oct. 2014.

[20] G. Templeton, “Dark market massacre: FBI shuts down silk road 2.0 and dozens more tor websites,” https://www.extremetech.com/extreme/193821-dark-market-massacre-fbi-shuts-down-silk-road-2-0-and-400-other-tor-websites, Nov. 2014, accessed: 2022-11-10.

[21] N. Woolf, “Bitcoin ’exit scam’: deep-web market operators disappear with $12m,” *The Guardian*, Mar. 2015.

[22] B. Krebs, “Dark web’s ‘evolution market’ vanishes,” https://krebsonsecurity.com/2015/03/dark-webs-evolution-market-vanishes/, Mar. 2015, accessed: 2022-11-17.

[23] A. Greenberg, “Agora, the dark web’s biggest drug market, is going offline,” *Wired*, Aug. 2015.

[24] B. Patrianakos, “Buying drugs online remains easy,” http://southwestcoalition.org/buying-drugs-online-remains-easy/, accessed: 2022-11-10.

[25] J. Leyden, “Dark web souks are so last year: Cybercrooks are switching to telegram,” https://www.theregister.com/2018/06/07/cybercrime_bazaar_to_telegram/, Jun. 2018, accessed: 2022-11-2.

[26] W. Tsing, “Wall street market reported to have exit scammed,” https://www.malwarebytes.com/blog/news/2019/04/wall-street-market-reported-to-have-exit-scammed, Apr. 2019, accessed: 2022-11-10.

[27] Europol, “Double blow to dark web marketplaces - europol press release,” May 2019.

[28] J. Pagliery, “FBI shuts down online drug market silk road,” https://money.cnn.com/2013/10/02/technology/silk-road-shut-down/index.html, Oct. 2013, accessed: 2022-5-31.

[29] B. Krebs, “Silk road lawyers poke holes in FBI’s story,” https://krebsonsecurity.com/2014/10/silk-road-lawyers-poke-holes-in-fbis-story/, Oct. 2014, accessed: 2022-6-27.

[30] C. Tarbell, “United states of america vs ross william ulbricht,” Sep. 2013.

[31] S. Thielman, “Silk road operator ross ulbricht sentenced to life in prison,” *The Guardian*, May 2015.

[32] A. Greenberg, “At least two moderators of ’silk road 2.0’ drug site forums arrested,” *Forbes Magazine*, Dec. 2013.

[33] Europol, “Operation onymous,” https://www.europol.europa.eu/operations-services-and-innovation/operations/operation-onymous, Nov. 2014, accessed: 2022-11-10.

[34] S. L. Chua, “Measuring the deterioration of trust on the dark web: Evidence from operation bayonet,” in *Workshop on the Economics of Information Security (WEIS), online*, 2021.

[35] S. Khandelwal, “Feds seize AlphaBay and hansa markets in major Dark-Web bust,” https://thehackernews.com/2017/07/alphabay-hansa-darkweb-markets-seized.html, Jul. 2017, accessed: 2022-6-27.

[36] R. Koenes and K. Voskuil, “Politie neemt deel darkweb over: honderden verdachten in beeld,” https://www.ad.nl/binnenland/politie-neemt-deel-darkweb-over-honderden-verdachten-in-beeld~ae77cb7f/, Jul. 2017, accessed: 2022-6-27.

[37] Federal Bureau of Investigation, “AlphaBay takedown,” https://www.fbi.gov/news/stories/alphabay-takedown, Jul. 2017, accessed: 2022-6-27.

[38] A. Greenberg, “Operation bayonet: Inside the sting that hijacked an entire dark web drug market,” *Wired*, Mar. 2018.

[39] D. Schouten and F. Tijmstra, “Drugskopers op dark web krijgen onverwacht politiebezoek,” *EenVandaag*, Feb. 2018.

[40] Telegram, “Telegram FAQ,” https://telegram.org/faq?setln=en, accessed: 2022-3-29.

[41] H. Saribekyan and A. Margvelashvili, “Security analysis of telegram,” Massachusetts Institute of Technology, Tech. Rep., May 2017.

[42] N. Maréchal, “From russia with crypto: A political history of telegram,” in *8th USENIX Workshop on Free and Open Communications on the Internet (FOCI 18)*, 2018.

[43] A. Tsotsis, “Telegram saw 8M downloads after WhatsApp got acquired,” *TechCrunch*, Feb. 2014.

[44] D. Hakim, “Once celebrated in russia, the programmer pavel durov chooses exile,” *The New York Times*, Dec. 2014.

[45] Telegram, “Admins, supergroups and more,” https://telegram.org/blog/supergroups, Nov. 2015, accessed: 2022-3-30.

[46] A. Dargahi Nobari, N. Reshadatmand, and M. Neshati, “Analysis of telegram, an instant messaging service,” in *Proceedings of the 2017 ACM on Conference on Information and Knowledge Management*, ser. CIKM ’17. New York, NY, USA: Association for Computing Machinery, Nov. 2017, pp. 2035–2038.

[47] P. Durov, “Durov’s channel,” https://t.me/durov/142, Dec. 2020, accessed: 2022-3-30.

[48] Telegram Team, “$300,000 for cracking telegram encryption,” https://telegram.org/blog/cryptocontest, Nov. 2014, accessed: 2022-11-17.

[49] D. Georgoulias, J. M. Pedersen, M. Falch, and E. Vasilomanolakis, “A qualitative mapping of darkweb marketplaces,” in *2021 APWG Symposium on Electronic Crime Research (eCrime)*, Dec. 2021, pp. 1–15.

[50] E. Nunes, A. Diab, A. Gunn, E. Marin, V. Mishra, V. Paliath, J. Robertson, J. Shakarian, A. Thart, and P. Shakarian, “Darknet and deepnet mining for proactive cybersecurity threat intelligence,” in *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*, Sep. 2016, pp. 7–12.

[51] N. Christin, “Traveling the silk road: a measurement analysis of a large anonymous online marketplace,” in *Proceedings of the 22nd international conference on World Wide Web*, ser. WWW ’13. New York, NY, USA: Association for Computing Machinery, May 2013, pp. 213–224.

[52] S. Pastrana, D. R. Thomas, A. Hutchings, and R. Clayton, “CrimeBB: Enabling cybercrime research on underground forums at scale,” in *Proceedings of the 2018 World Wide Web Conference*, ser. WWW ’18. Republic and Canton of Geneva, CHE: International World Wide Web Conferences Steering Committee, Apr. 2018, pp. 1845–1854.

[53] V. Benjamin, Arizona State University, J. S. Valacich, H. Chen, University of Arizona, and University of Arizona, “DICE-E: A framework for conducting darknet identification, collection, evaluation with ethics,” *Miss. Q.*, vol. 43, no. 1, pp. 1–22, Jan. 2019.

[54] D. Décary-Hétu and D. Laferrière, “Discrediting vendors in online criminal markets,” *Disrupting criminal networks: Network analysis in crime prevention*, pp. 129–152, 2015.

[55] W. Lacson and B. Jones, “The 21st century DarkNet market: Lessons from the fall of silk road,” Jul. 2016.

[56] A. Amarasingam, S. Maher, and C. Winter, “How telegram disruption impacts jihadist platform migration,” Eceonomic and Social Research Council, Tech. Rep., 2021.

[57] G. Weimann, “Terrorist migration to the dark web,” *Perspectives on Terrorism*, vol. 10, no. 3, pp. 40–44, 2016.

[58] V. Peter, R. Kühn, J. Mitroviç, M. Granitzer, and H. Schmid-Petri, “Network analysis of german COVID-19 related discussions on telegram,” *Natural Language Processing and Information Systems*, vol. LNCS 13286, 2022.

[59] th3unkn0n, “TeleGram-Scraper: telegram group scraper tool. fetch all information about group members,” 2020.

[60] PeterWalchhofer, “Telescrape: Telegram scraper for downloading messages, comments, users and photos,” 2020.

[61] M. Blankers, D. van der Gouwe, L. Stegemann, and L. Smit-Rigter, “Changes in online psychoactive substance trade via telegram during the COVID-19 pandemic,” *Eur. Addict. Res.*, vol. 27, no. 6, pp. 469–474, Jun. 2021.

[62] L. Moyle, A. Childs, R. Coomber, and M. J. Barratt, “#drugsforsale: An exploration of the use of social media and encrypted messaging apps to supply and access drugs,” *Int. J. Drug Policy*, vol. 63, pp. 101–110, Jan. 2019.

[63] H. Wang, Y. Hou, and H. Wang, “A novel framework of identifying chinese jargons for telegram underground markets,” in *2021 International Conference on Computer Communications and Networks (ICCCN)*, Jul. 2021, pp. 1–9.

[64] The Telegram Team, “Silent messages, slow mode, admin titles and more,” https://telegram.org/blog/silent-messages-slow-mode?setln=pl, Aug. 2019, accessed: 2022-12-20.

[65] ——, “Search filters, anonymous admins, channel comments and more,” https://telegram.org/blog/filters-anonymous-admins-comments/pl?setln=en, Sep. 2020, accessed: 2022-12-20.

[66] D. Lummen, K. Boersma, R. Dijkstra, and J. Sustronk, “Is telegram the new place to be for criminal?” Research Assignment, available upon request, Jun. 2021.

[67] M. van Volksgezondheid Welzijn en Sport, “Opiumwet,” https://wetten.overheid.nl/BWBR0001941/2023-01-01/0/informatie, Jan. 2023, accessed: 2023-1-13.

[68] National Strategic Group, “The psychology of customer reviews,” https://www.nationalstrategic.com/why-would-they-write-that-the-psychology-of-customer-reviews/, Jun. 2018, accessed: 2023-2-17.

[69] P. Nederland, “Politiebericht op telegram in phishingonderzoek,” https://www.politie.nl/nieuws/2022/augustus/3/10-politiebericht-op-telegram-in-phishingonderzoek.html, Aug. 2022, accessed: 2023-1-19.

Appendix A

Appendix

A.1 Additional Tables Goods & Services

	Wallstreet Market	Hansa Market	Alphabay Market
Weapons	0.00%	0.00%	0.15%
Firearms and Explosives	0.00%	0.00%	1.13%
Fireworks	0.00%	0.00%	0.00%
Licenses and Personal Documents	2.64%	3.30%	1.79%
Stolen Goods	1.50%	0.65%	1.46%
Soft Drugs	19.69%	22.78%	22.76%
Hard Drugs	22.07%	22.88%	19.80%
Pharmaceuticals	17.78%	15.23%	19.64%
Cashout	8.73%	5.48%	7.32%
Cybercrime	6.40%	17.19%	7.93%
Other	21.20%	12.49%	18.02%

Table A.1: Distribution of advertisement categories on Darknet Marketplaces, all advertisements

	Wallstreet Market	Hansa Market	Alphabay Market
Weapons	0.00%	0.00%	0.03%
Firearms and Explosives	0.00%	0.00%	0.21%
Fireworks	0.00%	0.00%	0.00%
Licenses and Personal Documents	0.51%	0.00%	0.02%
Stolen Goods	0.0%7	0.01%	0.03%
Soft Drugs	18.99%	37.89%	18.94%
Hard Drugs	55.95%	37.49%	44.82%
Pharmaceuticals	16.03%	22.98%	29.19%
Cashout	1.83%	0.41%	0.75%
Cybercrime	0.00%	0.02%	0.18%
Other	6.61%	1.20%	5.84%

Table A.2: Distribution of advertisement categories on Darknet Marketplaces, items shipping from NL

	Wallstreet Market	Hansa Market	Alphabay Market
Weapons	0.00%	0.00%	0.05%
Firearms and Explosives	0.00%	0.00%	0.09%
Fireworks	0.00%	0.00%	0.00%
Licenses and Personal Documents	0.97%	1.71%	2.53%
Stolen Goods	0.15%	0.03%	0.28%
Soft Drugs	20.25%	24.16%	12.41%
Hard Drugs	34.61%	31.54%	14.57%
Pharmaceuticals	13.96%	12.49%	10.27%
Cashout	16.74%	12.25%	28.15%
Cybercrime	4.73%	6.72%	9.64%
Other	8.59%	11.10%	22.02%

Table A.3: Distribution of advertisement categories on Darknet Marketplaces, all orders

	Ads	Non-Ads
Cashout-01	84.38%	15.62%
Cashout-02	82.19%	17.81%
Cashout-03	89.05%	10.95%
Drugs-01	67.09%	32.91%
Fireworks-01	50.56%	49.44%
Fireworks-02	36.71%	63.29%
General-01	68.35%	31.65%
General-02	75.69%	24.31%
General-03	74.60%	25.40%
General-04	76.15%	23.85%
General-05	86.01%	13.99%
General-06	82.67%	17.33%
General-07	78.43%	21.57%
General-08	84.10%	15.90%
General-09	88.04%	11.96%
General-10	85.92%	14.08%
General-11	8.88%	91.12%
General-12	83.83%	16.17%
General-13	84.78%	15.22%
General-14	79.36%	20.64%
General-15	81.02%	18.98%
General-16	85.86%	14.14%
General-17	80.31%	19.69%
General-18	86.32%	13.68%
Local-01	82.30%	17.70%
Local-02	83.74%	16.26%
Local-03	84.06%	15.94%
Local-04	85.26%	14.74%
Local-05	80.86%	19.14%
Local-06	79.15%	20.85%

Table A.4: Ads / Non-ads distribution over all messages in Telegram Groups

	Weapons	Firearms and Explosives	Fireworks	Licenses and Personal Documents	Stolen Goods	Soft Drugs	Hard Drugs	Pharma-ceuticals	Cashout	Cyber-crime	Other
Cashout-01	0.31%	0.31%	0.07%	9.41%	3.54%	11.48%	19.72%	5.51%	33.51%	14.21%	1.93%
Cashout-02	0.19%	0.15%	0.05%	11.66%	5.33%	6.13%	18.86%	3.61%	37.95%	14.69%	1.40%
Cashout-03	0.37%	0.04%	0.01%	11.34%	6.40%	3.78%	20.99%	4.49%	37.18%	14.81%	0.60%
Drugs-01	0.03%	0.24%	0.17%	5.10%	1.92%	33.89%	28.62%	2.79%	18.56%	4.12%	4.56%
Fireworks-01	0.09%	0.82%	75.84%	0.23%	1.59%	6.61%	3.77%	0.26%	6.77%	1.70%	2.32%
Fireworks-02	0.09%	0.84%	74.56%	0.20%	1.63%	6.52%	3.85%	0.26%	7.90%	1.97%	2.18%
General-01	0.15%	0.11%	0.03%	6.22%	3.30%	8.76%	34.41%	4.55%	33.93%	7.80%	0.75%
General-02	0.34%	0.33%	0.11%	2.63%	0.40%	16.15%	52.97%	10.54%	12.17%	3.35%	1.02%
General-03	0.28%	0.54%	0.28%	2.79%	2.49%	12.80%	43.87%	4.64%	20.44%	8.01%	3.85%
General-04	0.12%	0.32%	0.12%	4.74%	3.06%	16.17%	37.02%	9.13%	20.15%	7.78%	1.40%
General-05	0.23%	0.15%	0.07%	9.65%	3.75%	11.50%	29.81	5.40	29.81%	8.46%	1.19%
General-06	0.21%	0.16%	0.05%	11.79%	5.05%	6.37%	20.90%	3.71%	36.18%	14.05%	1.55%
General-07	0.30%	0.38%	0.03%	9.95%	2.49%	10.57%	26.96%	8.19%	29.03%	11.61%	0.49%
General-08	0.21%	0.18%	0.04%	14.56%	5.10%	5.59%	17.96%	3.72%	37.33%	14.07%	1.22%
General-09	0.28%	0.04%	0.02%	5.84%	4.18%	10.48%	32.30%	7.52%	28.32%	10.77%	0.24%
General-10	0.28%	0.13%	0.09%	8.42%	3.74%	11.48%	32.29%	18.92%	15.03%	8.44%	1.17%
General-11	0.01%	0.37%	0.36%	1.36%	1.49%	3.57%	3.54%	0.10%	50.70%	30.51%	7.98%
General-12	0.00%	0.18%	0.02%	7.22%	4.68%	14.69%	31.58%	6.64%	23.95%	9.55%	1.49%
General-13	0.23%	0.15%	0.04%	12.34%	6.14%	6.07%	19.28%	3.81%	35.59%	15.02%	1.33%
General-14	0.41%	0.47%	0.37%	2.39%	2.81%	14.01%	50.57%	9.39%	13.04%	4.83%	1.70%
General-15	0.36%	0.22%	0.04%	4.47%	6.41%	10.09%	27.26%	7.37%	34.26%	8.80%	0.72%
General-16	0.02%	0.70%	0.03%	7.56%	7.40%	19.81%	24.08%	10.82%	18.68%	10.02%	0.88%
General-17	0.02%	0.35%	0.11%	4.00%	0.29%	16.39%	53.46%	8.66%	14.44%	1.43%	0.85%
General-18	0.49%	0.18%	0.02%	10.85%	2.51%	15.22%	32.24%	2.24%	16.09%	18.59%	1.56%
Local-01	0.14%	0.16%	0.12%	8.66%	3.27%	11.77%	32.00%	10.47%	21.38%	10.91%	1.12%
Local-02	0.18%	0.11%	0.07%	8.25%	4.16%	11.47%	33.50%	4.78%	28.08%	8.50%	0.89%
Local-03	0.24%	0.06%	0.04%	9.36%	2.92%	12.32%	26.52%	4.45%	35.65%	7.54%	0.90%
Local-04	0.38%	0.09%	0.04%	8.19%	7.05%	11.82%	31.34%	10.02%	23.14%	6.46%	1.49%
Local-05	0.42%	0.17%	0.03%	9.72%	4.40%	16.01%	25.56%	7.03%	30.85%	5.07%	0.73%
Local-06	0.49%	0.20%	0.09%	9.34%	3.94%	14.03%	34.71%	12.77%	15.71%	8.04%	0.67%

Table A.5: Category Distribution over all messages in Telegram Groups

	Cashout	Drugs	Fireworks	General	Local
Weapons	0.29%	0.03%	0.09%	0.22%	0.31%
Firearms and Explosives	0.17%	0.24%	0.83%	0.28%	0.13%
Fireworks	0.04%	0.17%	75.20%	0.10%	0.06%
Licenses and Personal Documents	10.80%	5.10%	0.22%	7.04%	8.92%
Stolen Goods	5.09%	1.92%	1.61%	3.63%	4.29%
Soft Drugs	7.13%	33.89%	6.56%	11.65%	12.90%
Hard Drugs	19.86%	28.62%	3.81%	31.69%	30.60%
Pharmaceuticals	4.54%	2.79%	0.26%	6.96%	8.25%
Cashout	36.21%	18.56%	7.34%	26.06%	25.80%
Cybercrime	14.57%	4.12%	1.84%	10.73%	7.75%
Other	1.31%	4.56%	2.25%	1.63%	0.97%

Table A.6: Category distribution over all messages in Combined Telegram Groups

	Telegram Groups	Darknet Marketplaces
Weapons	0.23%	0.05%
Firearms and Explosives	0.27%	0.38%
Fireworks	5.10%	0.00%
Licenses and Personal Documents	7.28%	2.57%
Stolen Goods	3.72%	1.20%
Soft Drugs	11.85%	21.74%
Hard Drugs	28.33%	21.58%
Pharmaceuticals	6.39%	17.55%
Cashout	25.53%	7.18%
Cybercrime	9.70%	10.51%
Other	1.61%	17.24%

Table A.7: Category distribution for overall Darknet Marketplaces and Telegram Groups