Toad in the Hole or Mapo Tofu? Comparative Analysis of English and Chinese Darknet Markets

Abstract—The popularity of online shopping and cryptocurrency has contributed to drive the economy of darknet markets in recent years. These are often perceived to be conducive to (or may even facilitate) cybercrime related activities. It is, therefore, worthwhile to have a deeper understanding on how various darknet markets operate, so that researchers and law enforcement can test and deploy appropriate countermeasures to fight against online crime. Currently, there is a knowledge gap regarding the similarities and differences of English and Chinese based darknet markets. This study aims to compare between darknet markets operating in English and Chinese. Data from three English and two Chinese darknet markets was collected. The gathered data is described, compared, and analysed in six main aspects: operation model and structures, product categories, market policies, payment methods, security mechanisms, and vendors' characteristics. Our datasets were collected during a seven-week period between 17 July and 30 August 2021, and they contain data from 384 vendors in the English darknet markets and 4,429 in the Chinese ones. The Chinese darknet markets generally seem to have more liberal policies than their English counterparts, as demonstrated by the variety and types of goods and services offered, many of which would have been banned in the English speaking ones. All darknet markets suffer from reputation issues. Cross-market actors are active, but they represent only a small proportion of the vendors observed in our study. In summary, our findings reveal key characteristics of darknet markets in two widely used languages. This information can provide useful insights for security researchers and law enforcement agencies in combating cybercrime.

Index Terms—e-crime, cybercrime, darknet, anonymous online markets, vendors, comparative study, data collection.

I. INTRODUCTION

As the Internet became an integral part of everyone's lives, more and more people conduct business transactions online. The stakeholders include not only legitimate vendors and buyers, but also cybercriminals, who tend to engage in online trading to boost profits, evade capture and expand their criminal operations. Anonymous online markets – popularly known as *darknet markets* – have played a big role in the modern cybercrime ecosystem. The Onion Router (Tor) provides a key building block for enabling anonymous online markets. Tor is an open-source software that uses volunteer nodes for hiding its users' IP addresses through multiple hops [1]. Tor was initially used for privacy protection [2], but darknet markets also leverage the Tor network, in order to provide anonymity for their stakeholders. This poses some difficulties to law enforcement agencies in identifying and tracking the stakeholders involved, which include both cybercriminals and, at times, even victims.

In the past, the Silk Road was one of the first and most prominent darknet markets, but it was shut down in October 2013 [3]. The US government seized over $1 billion worth of bitcoin connected to the old Silk Road market [4]. Nevertheless, shutting down a market is not the end of the "game" for many of the operators. Vendors usually continue to trade on other platforms, at times after changing their username. As a trend, new markets will appear just weeks after others are closed, alternative, vendors and customers will move to already existing, smaller markets.

With the increasing number of markets in operation, it is important to study cybercrime stakeholders (such as cybercriminals and victims) comprehensively. Gaining in-depth insights from such an investigation will provide law enforcement agencies and security researchers with a clear understanding of the operation and the evolution of darknet markets, which in turn will enable the creation of appropriate countermeasures and mitigation techniques to combat cybercrime.

Previous studies have measured a wide range of darknet markets, but they are heavily skewed towards those conducting their business mainly in English. However, English darknet markets are not the only platforms of interest here. Investigations into other language darknet markets – such as those in Chinese or Russian – are still scarce, and this is a gap that needs to be addressed. Furthermore, and due to the rise of cryptocurrency despite their hard stance towards bitcoin, Chinese law enforcement has also increased their effort to fight criminal activities in darknet marketplaces [5]. The development and acceleration of economic globalisation have also made it necessary to study the diversity and impact of darknet markets in different regions of the world.

The study presented in this paper aims *to investigate, analyse and compare several current popular English and Chinese darknet marketplaces*. The main research question is whether there are key differences between marketplaces operating in English and those in Chinese. As a secondary research question, we would also like to know if such differences – assuming there are noticeable – would influence the behaviour of vendors and the market policies, as well as the characteristics of cross-market actors.

Contributions. We collected datasets from five active and popular darknet markets, three operating in English and two in Chinese. Through statistical analysis and in-depth investigation, we track some indicators and come up with a summary of key characteristics, and we study how these characteristics compare between the two different languages marketplaces. We described, analysed, and compared the results of our investigation in six main aspects: (i) operation model and

structures, (ii) product categories, (iii) market policies, (iv) payment methods, (v) security mechanisms, and (vi) vendors' characteristics. We share our insights into market development and vendors' behaviour, which are helpful for future investigations.

The rest of the paper is organised as follows. Firstly, we provide an overview of relevant related work in Section II. We then explain our approach and how we carried out our data collection, and we present an overview of the datasets in Section III. We show the results from different perspectives (including operation model and structures, product category, market policy, payment methods, security mechanisms, vendors' characteristics) in Section IV. We discuss the implications of such insights, along with the challenges and limitations of our study in Section V. Finally, we summarise the implication of this study and present our conclusions regarding the nature of cybercrime in darknet markets in Section VI.

II. RELATED WORK

Several prior works studied darknet markets and forums. Christin [6] performed a comprehensive measurement analysis of the Silk Road, showing that drugs were the main concern. The paper also estimated the overall market profit and possible intervention methods. Wegberg et al. [7] tracked the evolution of commoditisation on eight English darknet markets over six years. The paper concluded that retail has a large share in the darknet markets, and the overall revenue for cybercrime commodities was $15 million between 2011 to 2017. More recently, Vu et al. [8] described the evolution of the Hack Forums marketplace through the set-up, stable and Covid-19 pandemic eras. They found that the market centralised heavily around influential users and threads.

There are other studies focused on identifying the characteristics of key actors, which can then be used to obtain more insights and to understand the cybercrime ecosystem [9] [10] [11] [12] [13] [14] [15]. More specifically, Yip et al. [16] examined the structure of organised cybercrime by quantitative analysis of data coming from online underground markets. The paper concluded that trust is an important factor in promoting the prosperity of the underground economy. Holt [17] described the relationship between actors influenced by the price, customer service, and trust in ten Russian underground forums through a qualitative investigation, focusing on malware and attack tools. Bhalerao et al. [18] tried to identify supply chains from major English and Russian cybercrime forums.

However, there is still limited research looking into how different language darknet markets compare. Zhou and Zhuge [19] analysed and described the differences in darknet markets between Chinese and English speaking communities. They mainly looked at three aspects: market operation, security, and goods sales. They also described the difference in selling goods depending on relevant laws and regulations. Our work has been informed by this study. We have included more comprehensive data about the English and Chinese darknet markets under study regarding market policies, payment methods, crawling restrictions, and some vendor's indicators and

main characteristics. We also found a new type of trading model in a Chinese darknet market, namely the "request-to-buy mode". Our datasets also contain the most recent descriptive information, such as product posts and vendor profiles, which can be valuable for analysis purposes and are available to any law enforcement or academic researcher, after proper identification.

Most of the publicly available datasets for darknet markets are out of date. These include the 2016 and 2017 DreamMarket datasets from AZSecure-data [20]. The Dark Net Market archives from 2011 to 2015 by Branwen et al. [21] is another example of useful, but quite out of date dataset. CrimeBB is the only dataset that is still maintained and updated by the Cambridge Cybercrime Centre [22]. The dataset included one underground forums containing roughly 180,000 contracts. However, we decided to do our own data collection due to the more specific types of data that we would need, namely specific languages constraints and continuous data spanning several weeks.

III. METHODOLOGY

This section outlines our approach and provides an overview of the data collection process, including the description of the two crawling mechanisms, a detailed outline of our datasets[1], and the specific details of the technical environment. We also briefly discuss ethical considerations at the end of this section.

A. Approach

In order to understand how different language darknet markets work, we carried out a study based on a combination of observational, retrospective, and longitudinal approaches [23]. We constructed our datasets during a seven-week period between 17 July and 30 August 2021, containing data from 384 vendors in the English darknet markets and 4,429 in the Chinese darknet markets. We analysed these data regarding six different aspects: (i) operation model and structures, (ii) product category, (iii) market policy, (iv) payment methods, (v) security mechanisms, and (vi) vendors' characteristics.

Data on the operation model and structures include the markets' basic information, as well as changes in the market size and the possible reasons behind such changes. The product category displays the proportion of different types of items in the markets based on the average number of each snapshot. The more comprehensive data available in the Chinese darknet markets means we can also estimate the revenue generated by the main product categories. The market policy mainly focuses on what goods or services are explicitly banned. The payment methods describe what currencies are accepted. The security mechanisms describe the crawling restrictions in each darknet market, as well as general account security. In terms of vendors' characteristics, we analysed vendor location, trust level and active/inactive status and time. We also selected some top and cross-market vendors in the English darknet markets,

---

[1]Due to the potentially criminal nature of the datasets, we have to choose an appropriate and ethical way for sharing them. We are happy to share our datasets with academics, security researchers, and law enforcement agencies.

TABLE I: Summary of the Observed Darknet Markets

Market	First seen	# Listings	# Vendors	Lang
Dark0de Reborn	2020-05	45876	1648	EN
White House Market	2019-08	44740	3453	EN
Cartel Marketplace	2020-06	2596	195	EN
Chinese Exchange Market	2018-03	10949	2636	CN
Tea Horse Road	2020-04	8302	1793	CN

and some top vendors in the Chinese darknet markets. We define top as the ones that make more profits, have more sales and have more positive feedback or better reputations during the observation period. Finally, we highlight some stark differences between English and Chinese darknet markets based on the six aspects above.

B. Data Collection

We used Python with the Scrapy web-crawling framework [24] to implement a custom crawler. Depending on the restriction policies of different markets and the information contained in each market, we used two sets of strategies:

1) If the market had stringent anti-crawl measures, the website would take a long time to crawl, or/and the session might expire during crawling. In this case, we would only collect data based on what is shown on the website home pages. For instance, most websites display highly rated vendors, promotional products and featured listings. Therefore, we could get selected vendors' data.

2) If the market had less stringent protections and restrictions, we would try to get as much information as possible through the listing pages.

The listing page URLs can usually be traversed easily in both strategies because their URLs are generally sequential. The product pages and vendor pages are partly obtained and parsed depending on the darknet marketplace website structure. Crawling restriction details are described and compared further in Section IV.

We collected datasets from five active and popular darknet markets, three operating mainly in English and two in Chinese. In order to ensure consistency and the validity of the research, we selected the same seven-week period between 17 July and 30 August 2021 for both sets of markets/languages. The data was collected once a week to avoid stressing the markets' website and being as inconspicuous as possible. In some circumstances, e.g. a DDoS attack on the website, the data collection was slightly delayed.

Table I provides a summary of the observed darknet market names, when they were first seen, the number of active listings of products, the number of active vendors, and the language used. The active numbers are as of 30 August 2021.

Dark0de Reborn is one of the English-based darknet markets, and it started in the early days of the Covid-19 outbreak, 24 May 2020. It has the most number of listings, and vendors are able to import feedback scores from other popular markets. Therefore, it has attracted a large number of vendors with good reputation. The market has strict crawling restrictions. We focus on the top vendors and collect data

from their product pages. Data include the vendors' profile pages and some of the feedback received. Meanwhile, we also collected some statistical data to study market trends. Technically, the crawler first gets the list of vendors usernames on the homepage. The vendors' profile pages are obtained through the fixed format of the URL.

White House Market is one of the most popular darknet markets in English language. The market has been in operation since 24 August 2019. A decline in Empire Market's reputation led to a rise of White House Market [25], which has a very high reputation. It also has the strictest crawling restrictions. We were only able to collect top vendors mentioned on the homepage and some statistical data. Data includes vendors' profile pages and the listing of products they currently sell. Technically, the crawler first obtains the list of vendors' usernames on the homepage. The vendors' profile pages and their listing pages are obtained through the fixed format of the URL, respectively. The listing may contain multi-pages. We used the `<div>` tag to determine whether there is another page to ensure the coverage of collected data.

Cartel Marketplace is a medium size darknet market in English. Although it is not as large as the previously mentioned markets, it still has a good reputation in dark web forums. So we think it should be included in the research. It has a relatively less stringent crawling policy. The product URLs are more likely random or coded, which means we had to traverse the whole listing with the page numbers. We saved all product URLs in a list, then sent requests accordingly. We were able to collect all vendor's information in this market.

Chinese Exchange Market is the most active and oldest darknet market in Chinese. It was developed from a forum. It has a less stringent crawling policy, and the cookie structure is also very simple. Therefore, we collected all active listing pages and parsed them. Technically, the product URLs are sequential. It can be traversed easily using a brute force approach.

Tea Horse Road is representative of the new generation of Chinese darknet markets. It has a user-friendly interface with an innovative "request-to-buy" model. It is a market with several historical versions, the earliest can be traced back to October 2019. The current version of the market launched around April 2020. It also has a less stringent crawling policy, although the structure of cookies is a bit complicated. We managed to collect all active listing pages because the product URLs are, again, sequential so they can be traversed exhaustively.

Table II provides a comparison of the indicators and features of the collected markets. The data marked as ✗ means either the indicator does not exist in the market or it was not collected due to crawling limitations.

C. Technical Environment

We connected to the Tor network using a Virtual Machine (VM) for a secure and anonymous access to the darknet markets. The VM runs Ubuntu 20.04.2.0 LTS with four cores, eight-thread, 8 GB RAM, 200 GB storage capacity and NAT
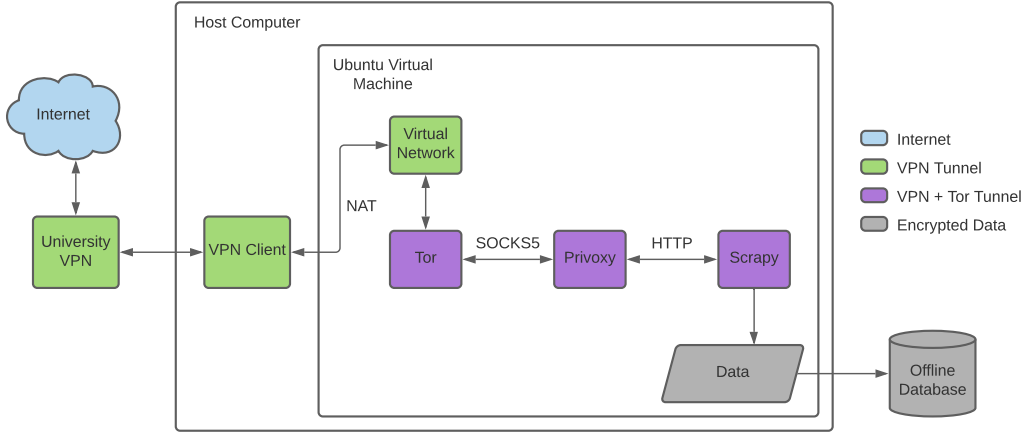
Fig. 1: The Set-up of Our Data Collection Scheme

TABLE II: Comparison of the Indicators and Features of the Collected Markets

		Dark0de Reborn	White House Market	Cartel Marketplace	Chinese Exchange Market	Tea Horse Road
Vendor Characteristics	Username / ID	✓	✓	✓	✓	✓
	Profile	✓	✓	✓	✗	✗
	Member Since	✓	✓	✓	✓	✗
	Last Seen	✓	✓	✓	✓	✗
	Total #Sales	✗	✓	✓	✓	✓
	Rating	✓	✓	✓	✗	✗
	Disputes	✗	✓	✓	✗	✗
	Feedback	✓	✓	✗	✗	✗
	PGP	✓	✓	✓	✗	✗
	#Listing	✓	✓	✓	✓	✓
Product	Title	✓	✓	✓	✓	✓
	Price	✓	✓	✓	✓	✓
	Category*	✓	✓	✓	✓	✓
	Sales	✓	✗	✓	✓	✓
	Shipping From	✓	✓	✓	✗	✗
	Shipping To	✓	✓	✗	✗	✗
Market	Total #Vendors	✓	✓	✓	✓	✓
	Total #Products	✓	✓	✓	✓	✓
	BTC	✓	✗	✓	✓	✓
	XMR	✓	✓	✓	✗	✗
	Fiat Currency	✗	✗	✗	✗	✓
	CAPTCHA	✓	✓	✓	✓	✓
* This is not for each product, but as an overall number.						

network from the host computer. VPN is used as a second security layer. To ensure our crawling was not detected, the `stem` library[2] was used for changing the Tor circuit every time we got a non-200 response code. We noticed that some researchers chose to change the Tor circuit frequently. We believe this will reduce efficiency and cause further stress to the market, because the cookies used for the request are the same but have different associated IP addresses. Since Tor uses SOCKS5 proxy and Scrapy uses HTTP proxy, Privoxy[3] is used to relay Tor and Scrapy. Once collected, the data was encrypted and saved into offline devices. Figure 1 shows the set-up of our data collection scheme.

D. Ethical Considerations

Since our study collected data from activities that could potentially be related to cybercrime – such as drug dealing,

[2]https://stem.torproject.org/
[3]https://www.privoxy.org/

sexual abuse and exploitation of vulnerable groups and other criminal activities – we had to make sure that we obtained ethical clearance before we commenced our study. The ethics for this study have been reviewed and approved by our university's Research Ethics Advisory Group.

IV. RESULTS

In this section, we present the results of our comparison for the darknet markets in English and in Chinese. The findings are divided into market, vendors, market policies, payment methods and security mechanisms.

A. Darknet Markets in English

1) Market: **Operation structures.** All three English darknet markets have a website interface similar to Silk Road. Figure 2 shows the Dark0de Reborn homepage. They all have multiple sections on the homepage, including promotional products, trending products and recommended top vendors.
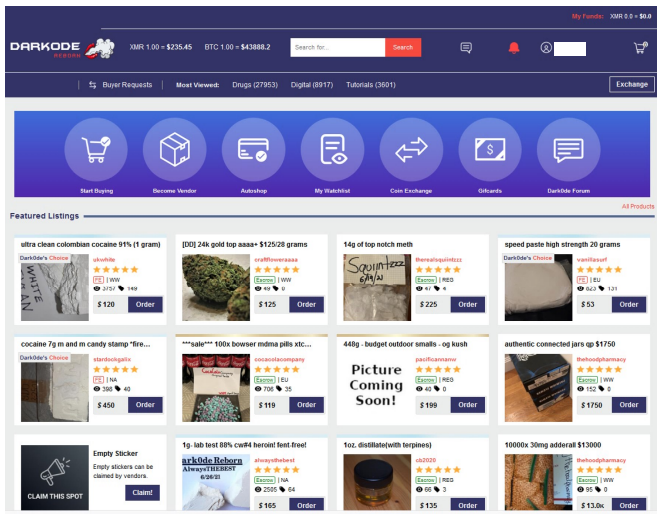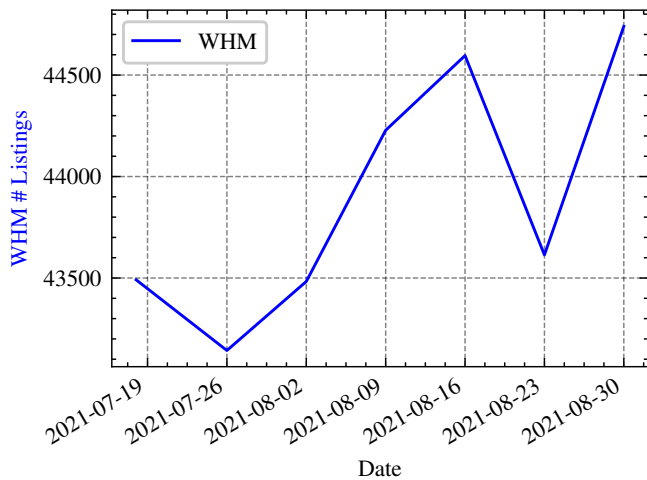
Fig. 2: Dark0de Reborn Homepage

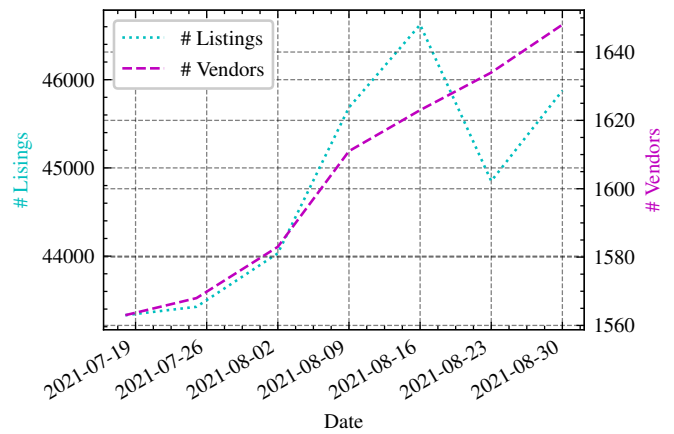Fig. 3: Number of Listings in White House Market

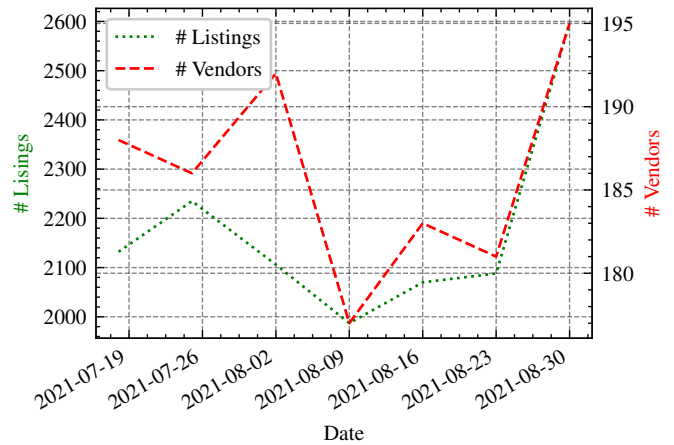Fig. 4: Number of Listings and Vendors in Dark0de Reborn Market

Fig. 5: Number of Listings and Vendors in Cartel Marketplace

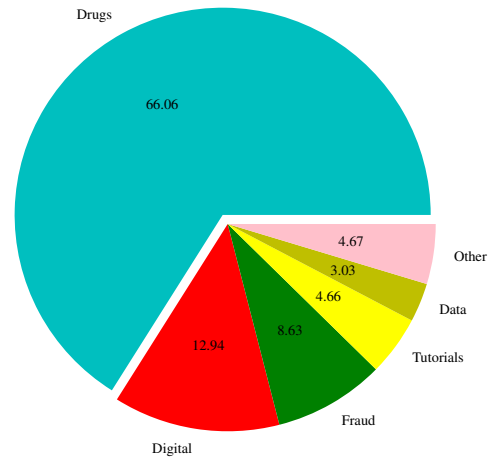Fig. 6: Breakdown of Categories in English Darknet Markets

There is usually a category list on the homepage, and users can browse all products under this category. Most web pages also support a mobile-friendly interface.

Number of listings and vendors. The number of listings and vendors indicates the state of a market. Figure 3 shows the number of listings in the White House Market (WHM) between 18 July and 30 August 2021[4]. Figure 4 shows the number of listings and vendors in the Dark0de Reborn. The overall listing number keeps rising, accompanied by some fluctuations in both markets. The White House Market and the Dark0de Reborn introduced a new Product Quality and Harm Reduction Program on 17 June 2021. The program aims to provide high-quality products and lower levels of risk to buyers. Vendors who send products and receive positive test results can get badges and display them on the product page to increase credibility, facilitate trust and increase sales. Also, the

vendors can apply for a reduced fee on White House Market if they test regularly. This program causes some non-compliant products to be removed. Figure 5 shows the number of listings and vendors in the Cartel Marketplace over the observation period. Those two lines are consistent in most weeks. As the number of vendors increases, the number of listings also rise.
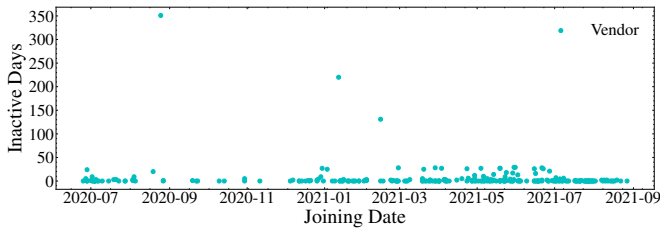
---

[4]The vendor information on the WHM is shown only in real-time, hence we do not have historic information on the number of vendors on the WHM. Furthermore, in early May 2021, the WHM stopped accepting any new vendors applications, making the number of vendors and the number of products offered to plateau. In comparison, the Dark0de Reborn maintained a continuous vendor growth.

Fig. 7: Inactive Days and Joining Date in Cartel Marketplace

TABLE III: The Proportion of Vendors' Locations in English Darknet Markets

Location	Number	Percentage
United States	124	32.29%
Worldwide	65	16.93%
United Kingdom	38	9.90%
Europe	37	9.64%
Netherlands	32	8.33%
Germany	19	4.95%
Australia	19	4.95%
N/A	11	2.86%
France	7	1.82%
North America	7	1.82%

Product category. Figure 6 shows that drugs take the largest proportion of the three darknet markets. We count those by using the website information listed in the navigation interface. Drugs account for over 66% of products, followed by digital products and fraud related materials. Digital products contain pirated software, exploit kits, digital services (DDoS services), botnets and malware. Another category of trending products in all three markets is physical items such as smart devices, jewellery, and watches. According to the vendors' descriptions, most of them are fakes or reshipping drops.

2) Vendor: **Inactive days.** Figure 7 shows the joining date and inactive days of 264 vendors from the Cartel Marketplace. We define the number of inactive days as the number of days from the last seen date to the date when the data was collected. A few vendors were not very active over 50 days, but most vendors were still active, even if they have been registered for more than one year. More than 89% of the vendors have appeared within ten days. Even though the total number of vendors in the market is small, they seem to be very active.

Location. In all three English darknet markets, we collated the location of 384 vendors based on their profiles. Table III shows the top ten countries and regions where those vendors are located, covering 359 vendors, or 93.49% of the 384 vendors. The United States and Europe are the main supply locations. Approximately 62% of European vendors are from the United Kingdom, the Netherlands and Germany. This result is consistent with previous reports [26]. In terms of Worldwide or N/A, this means that some vendors do not want to reveal their location, particularly when they only sell virtual items. According to observations on dark web forums, buyers tend to buy drugs in local countries and regions to reduce the risk of being discovered by customs and law enforcement agencies. Therefore, we have reason to believe that the location information provided by the vendor is mostly accurate, in order to better attract target customers.

Trust Level. This is usually the way to show the credibility of vendors in the English darknet markets. Figure 8 shows the relationship between trust level and sales, feedback, number of disputes and joining date in the Cartel Marketplace. The numbers displayed are the median value at each level. For example, in level 10, the median sales volume is 104. Level changes are affected by a combination of these four aspects. High-level vendors usually have higher sales volumes and better reviews. The duration of registration has a limited impact on the level reached. For example, *Vendor_EN_1* is a level 10 vendor who joined the market in July 2021 with 185 sales, only one dispute, and 141 positive feedbacks. Please note that not all orders compulsorily require feedback. On the contrary, *Vendor_EN_2*, trust level 5, joined the market in March 2021 with 526 sales but 15 disputes and only 187 positive feedbacks. As a result, in addition to sales, the number of complaints and positive feedback are also determinant to compute the trust level.

Behaviour. We selected some vendors to describe and analyse their behaviours from the White House Market. *Vendor_EN_3* joined the market in July 2020, and there are currently 3,680 sales with 95% positive feedback. In the seven weeks included in our datasets, the number of orders was at least 830. The vendor had over 7,000 transactions in the previous Empire Market, with 99% positive feedback. This vendor mainly sells cocaine products in the United States. The largest display unit can reach 500 grams, and the price is close to $20,000. According to the smallest sales unit, we calculate that his lowest total estimated profit is above $2.7 million with around $207,500 over the observation period. As a successful big vendor, they can usually use their name as a symbol of their brand. *Vendor_EN_4* also confirms this point. The vendor has good reviews in its own region and sells drugs in multiple darknet markets simultaneously. Most successful vendors sell in different English darknet markets at the same time. They use the same format and language style in their profile. Since the feedback rating of English darknet markets can be imported into another, buyers can easily identify cross-market vendors. Some vendors will also regularly update the product or their own situation in their profile. This can be used as a signal if they do not appear for a long time. They may be arrested or just quit, warning past and potential customers that they may be at risk.

3) Market Policy: In this subsection, we describe what products are banned on the three darknet markets in English. We also mention the regulations regarding communication between users.

In Dark0de Reborn, the policy is called "selling policies and seller code of conduct". It is strictly forbidden to sell any images of sexual abuse of children, Fentanyl related products and any product or service related to terrorism. Fentanyl is an analgesic generally used in surgery; excessive use can quickly lead to addiction, hypotension and death due to respiratory depression. The website stipulates the use of in-site messenger as the means of communication between buyers and sellers and for customer service. Also, the exchange of large amounts
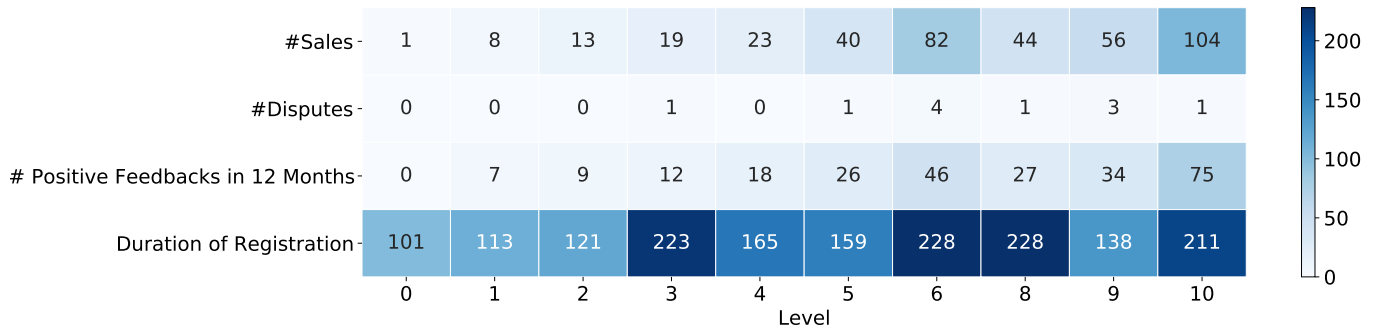
	0	1	2	3	4	5	6	8	9	10
#Sales	1	8	13	19	23	40	82	44	56	104
#Disputes	0	0	0	1	0	1	4	1	3	1
# Positive Feedbacks in 12 Months	0	7	9	12	18	26	46	27	34	75
Duration of Registration	101	113	121	223	165	159	228	228	138	211

Level

Fig. 8: Trust Level Correlation Matrix in Cartel Marketplace

(a) Dark0de Reborn CAPTCHA   (b) White House Market CAPTCHA   (c) Cartel Marketplace CAPTCHA
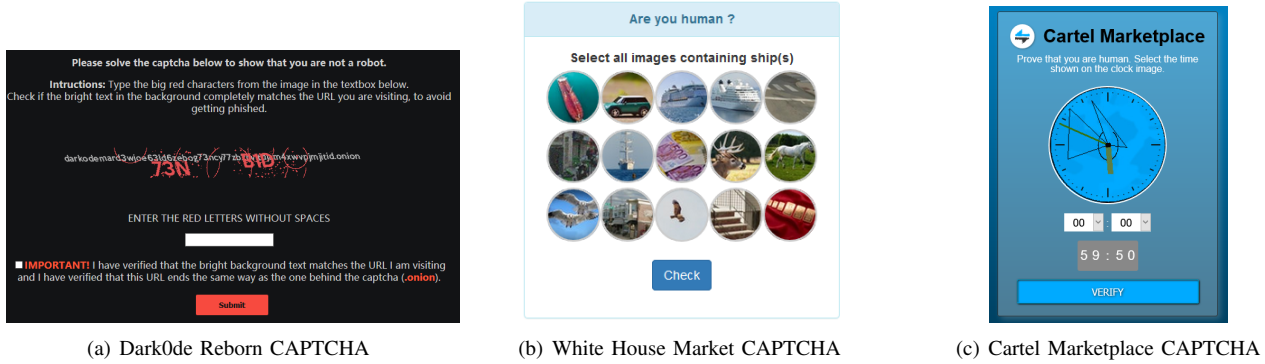
Fig. 9: CAPTCHA Samples from English Darknet Markets

of communications should be avoided unless paid for via Dark0de's services. To protect the competitiveness and security of the market, external links and external dissemination of user information are not allowed.

In comparison to Dark0de Reborn, the White House Market is more comprehensive and detailed. The policy strictly forbids any child abuse, human or animal abuse, murder for hire, weapons, Fentanyl and terrorism-related products. During the Covid-19 pandemic, products that purportedly can cure the virus are banned, but discounts on related tests and promotional codes are available. In terms of communication, they also bans external links and any external contact information.

At the Cartel Marketplace, the market rules are tough. The policy forbids child abuse, biological, radiological, or chemical weapons, murder for hire, scamming or deceptive tutorials. Searching for and publishing private or identifying information is not tolerated. In terms of communication, the website bans direct deals but does not limit external links or contact.

4) Payment Method: In all three markets, they use the on-site wallet mode. The user will be given a deposit address, then add funds by using Bitcoin or Monero. The Dark0de Reborn and Cartel Marketplace can use both Bitcoin and Monero. In the White House Market, since Bitcoin is much easier to track, only Monero is allowed, for security reasons. In the Dark0de Reborn, users can also use the website balance to purchase gift cards and send them to other accounts. That means the Dark0de Reborn supports the transfer of funds within the market. On the website, the default currency is USD. However, the user can choose between CAD, EUR, GBP, RUB, AUD, etc. The website also displays real-time market exchange rates.

Fig. 10: Chinese Exchange Market Homepage

5) Security Mechanisms: All three markets that we studied have strict crawling restrictions. In terms of CAPTCHA, Figure 9 shows the CAPTCHAs in English darknet markets. The Dark0de Reborn only implements a simple letter and number combination verification code. In the White House Market, the bot check consists in choosing the images that match the description out of 15 pictures. Those are randomly rotated, for added security. In the Cartel Marketplace, the user needs to indicate the time shown by the analogue clock. Then, there is another simple verification code to be filled in when login. The White House Market and Cartel Marketplace allow

users to choose how long the session will be kept alive at login pages. Available options are from ten minutes to 48 hours. After those verification processes, the user accesses the market's home page.

The number of pages that can be accessed per minute or hour is strictly limited, as well. The White House Market only allowed a limited number of requests in ten minutes. Even as a human, if the user tries to open multiple tabs at once, it is easy to trigger the detection system which will force logout and require re-login. Moreover, the trigger conditions may vary, and as such approximately 40 requests are allowed within 30 minutes. We applied a dynamic delay of 16 seconds to 90 seconds with six accounts. In the Cartel Marketplace, the limit of requests is 300 pages per session within about 40 minutes to 50 minutes. Once the user reaches such a threshold, the session expires automatically. We applied a dynamic delay of three seconds to ten seconds with three accounts. For the Dark0de Reborn, the threshold is unclear. We noticed a large number of requests that cannot be paralleled in the crawl and applied a dynamic delay of 5 seconds to 60 seconds. In terms of the structure of cookies, they seem to be static in all three markets, which means the cookies of a session do not change.

In terms of the user account, all three marketplaces use PGP public key to ensure account security. Once the user sets up the PGP public key in their profile, they are able to use Two-Factor Authentication (2FA). PGP has also been used widely in on-site communications. At the registration stage, the user needs to set up a username and password, and then the markets will send a set of English words to create a wallet.

B. Darknet Markets in Chinese

1) Market: **Operation model and structures.** In the Chinese Exchange Market, the website structure is simple and similar to a community forum. Figure 10 shows the Chinese Exchange Market homepage. It displays the latest posts under each category on the homepage. On each category page, each post contains the title, price, post time and vendor. In the Tea Horse Road, the interactive interface is more modern, and users can also browse by category. The Tea Horse Road also supports the request-to-buy mode, where users post the products they want to buy and describe their requisites, then vendors can provide quotes. Even though the structure of the two websites is relatively simple, the user experience is good, there are no redundant functions, and the products are easy to browse based on their category.

Number of listings and vendors. Figure 11 and Figure 12 show the number of listings and vendors over the observation period. In terms of the number of listings, both markets maintain an overall upward trend. Due to the operating mode of both, once the advertisement is posted on the website, the post will be kept for a long time even if the vendor is not active. Moreover, according to the data, the number of vendors remains stable. Even if the number of listings keeps growing, the number of vendors remains at a certain level. A new vendor may bring more than one listing.
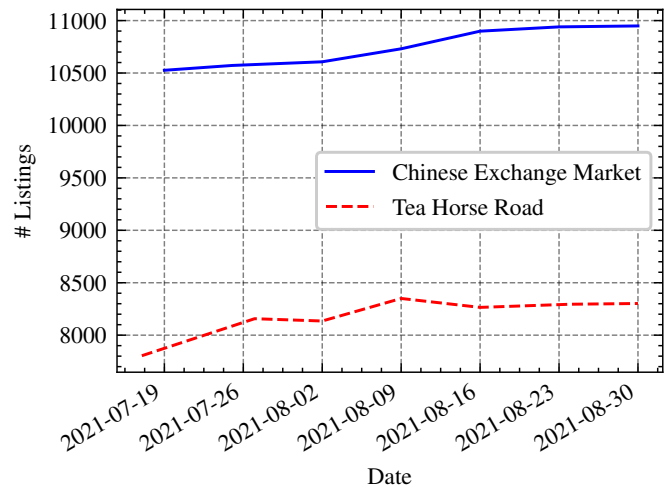

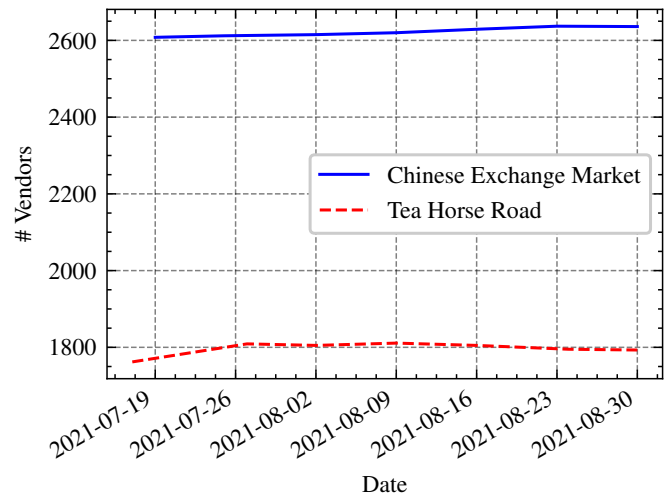Fig. 11: Number of Listings in Chinese Darknet Market

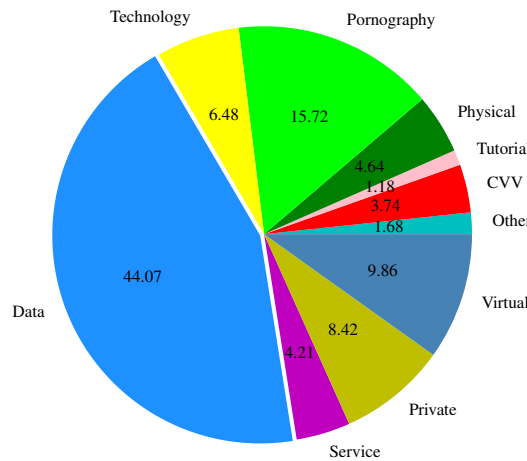Fig. 12: Number of Vendors in Chinese Darknet Market

Fig. 13: Breakdown of Categories in Chinese Exchange Market

Product category. Figure 13 shows the percentage of items that belong to each category in the Chinese Exchange Market. Leaked data and personal information accounted for the largest proportion, which is 44.07%. Pornography is the second most
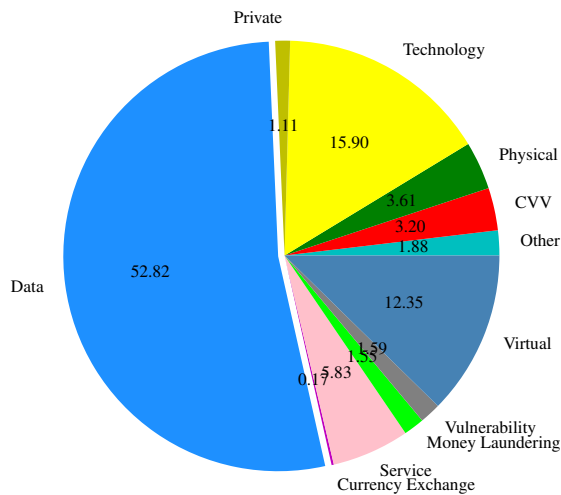
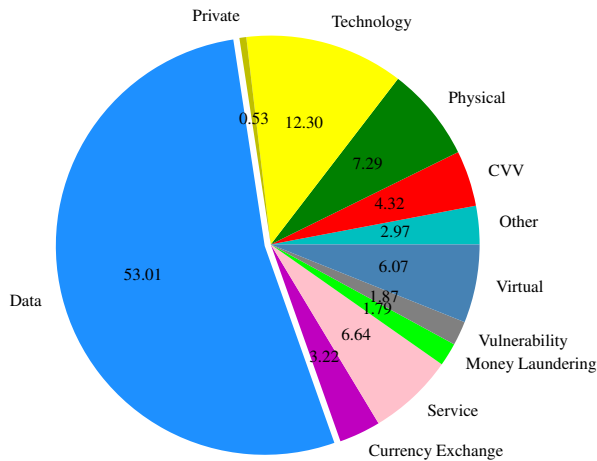Fig. 14: Breakdown of Categories in Tea Horse Road with Sale Mode

Fig. 15: Breakdown of Categories in Tea Horse Road with Request-to-Buy Mode
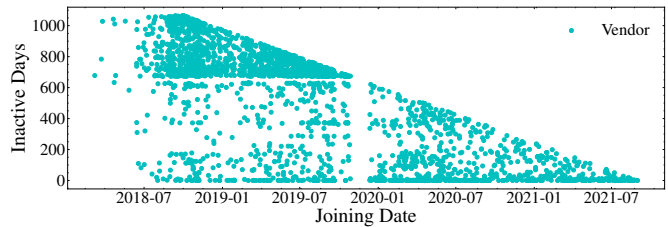

Fig. 16: Inactive Days and Joining Date in Chinese Exchange Market

graphic except private section, because the private section is usually priced in the smallest unit, which causes the sales number to be inaccurate. The pornographic category generated 1489 sales with $10,211.75 profits during the observation period. In the Tea Horse Road, the sales volume is displayed only within a certain period instead of cumulative (that is, the numbers count to this period will be deleted after a certain period of time), so the estimated profit is not as accurate.

2) Vendor: **Inactive days** Figure 16 shows the vendors' joining date and inactive days from the first post to the last seen in the Chinese Exchange Market with 2,537 vendors. At the end of 2019, there is a clear dividing line. We speculate that the market was maybe temporarily closed, banned many vendors, scam exited or updated for a long period of time. It seems like a large number of vendors exited the market at this point. Only a small part of the vendors before the end of 2019 have survived to present times, and some vendors that joined after 2020 are still active nowadays. After 2020, some people remained active until now.

Behaviour In both Chinese darknet markets, we selected some typical vendors to describe their behaviours. *Vendor_CN_1* has 113 sold items over a month with $6,773 estimated profits. The vendor first posted in June 2019, and generated a total of $29,021 in estimated profits. The vendor lists 88 posts about personal data, including pornography, virtual items and CVV related items. This personal data contains express delivery information in China, Japanese phone numbers, a set of Chinese ID card numbers with names, phone numbers and emails, email accounts with plaintext passwords, personal information in loan databases, motor vehicle registration information and much more, covering data all over the world. Pornography includes child abuse and hidden camera shots. Virtual items include VPN accounts and software. The CVV related items include card information and carding methods. In almost all posts, this vendor has screenshots to augment trust.

Vendor_CN_2 also sells personal data. The vendor sold 59 items with $2,124 estimated profits over the observation period. The most valuable product is the records of student data who attend university. The personal data contains name, age, phone number, e-mail address, school name and subject. *Vendor_CN_3* and *Vendor_CN_4* also provide services for whoring and hiring to hurt, respectively. However, there is not too much information in their posts, but they recommended using on-site communication for details. Since they do not have a clear price, the profit is difficult to estimate.

sold category with 15.72%, which includes child abuse. Private is a category that allowed buyers and vendors to use the market as the secured way to carry out their transaction. They usually have previously communicated and agreed to a deal.

Two figures show the percentage of each category in all items in the Tea Horse Road. Figure 14 shows the normal selling mode section. Figure 15 shows the request-to-buy mode section. Leaked data and personal information accounted for the largest proportion in both sections, approximately 53%. Pornography is classified as virtual items, and drugs are classified as physical items. Buyers request more physical items for sale.

In the Chinese darknet markets, the most profitable category is related to leaked and personal data. In the Chinese Exchange Market, all vendors are estimated to have made profits of at least $86,984.98 during the observation period. The profit related to personal data is $35,749.21, or 41.1% of all profits. The second is service, which usually are personal information query services or hires to harm others. Following is porno-

Fig. 17: CAPTCHA Samples from Chinese Darknet Markets

3) Market Policy: In the Chinese Exchange Market, there is no official policy pages just user instructions. As a guarantee intermediary, the market operation does not prohibit any products or services. Tutorials explain why vendors cannot do this by themselves and describe the potential risks. Otherwise, they will not be allowed to advertise. In a prominent position on the website, it is reminded that external connections and external communications are not allowed. Tea Horse Road forbids child abuse, unethical resources, materials to subvert state power, and political and political leaders related resources. In terms of communication, the website allows users to use off-site communication but avoid off-site transactions. Also, the website does not explain whether it is possible to use external websites, but we did found clean net links and other external websites in some product descriptions.

4) Payment Method: In the Chinese Exchange Market, the on-site wallet mode is used. The user needs to transfer Bitcoin to the Bitcoin wallet of the market administrator. The corresponding amount will be shown in their account on the market. On the advertisement post, the price is displayed in USD and Bitcoin. Tea Horse Road also uses the on-site wallet mode. The market allowed adding credit to their wallet by Bitcoin and Tether. Moreover, a difference with the Chinese Exchange Market is that users are allowed to use common fiat currency with daily payment methods, including Alipay, Wechat, and even debit cards, by contact market-authorized exchange via Telegram. On the advertisement post, the price is displayed in USD and Bitcoin.

5) Security Mechanisms: In both Chinese language markets, the crawling restrictions are easy to bypass. Both use simple four character letters and numbers combination CAPTCHAs when login-in. Figure 17 shows the CAPTCHAs in both Chinese darknet markets. Both markets lack request limitations. In order to avoid any bandwidth stress, we also applied a dynamic delay of 0.5 seconds to 2 seconds with a low number of concurrent requests. Hence, this causes the total crawling time to vary from four hours up to 12 hours. In terms of the structure of the cookies, the Tea Horse Road uses a dynamic approach in which it will change every time a request is sent. It does not seem to affect the crawling process, but

was noticed when setting up the initial cookie and we let the program follow up. We also noticed that the post page URLs are consecutive. This may lower the website's security level because of the potential for exhaustive cracking and crawling. Overall, both markets have low level crawling restrictions.

In terms of the user account, the two Chinese darknet markets have different mechanisms. In the Chinese Exchange Market, the user only needs to set a password. Then the website will assign an ID to the user. Interestingly, this user ID is a counter, which means that every time a new account is registered, the ID is increased by one. We tracked back our dataset and found that the ID is very likely to increment by 1. Our latest data shows that this ID is currently 677653. Although this is certainly not the number of active users in the market, it is the cumulative number of registered users in the market since its inception. The user needs to subscribe to the "post" and "reply" types of activity, respectively, to post and buy. The "post" cost 0.00024 and 0.0006 Bitcoin for three months and one year, respectively. The "reply" cost 0.00012 and 0.0003 Bitcoin for three months and one year, respectively. In the Tea Horse Road, the user needs to set a username, password and payment password. The payment password is used when a user purchases a product. Accounts need to be activated before publishing or purchasing products. The user needs to pay $10 in equivalent Bitcoin for the activation. There are no account password recovery options in either market.

C. Comparison of Darknet Markets in English and Chinese

The differences between the Chinese and English darknet markets are reflected in many aspects. This section is divided into two subsections to describe the market and vendors characteristics.

1) Market: **Operation model and structures.** English darknet markets tend to be a real online market, while Chinese darknet markets tend to be more similar to forums. Some built-in functions in the English darknet markets, such as credit systems, feedback systems, build a mature ecosystem. In the Chinese darknet markets, they only serve as an intermediate platform for posting. It is, therefore, quite difficult for users to judge the credibility of the vendor. In terms of novelty, one of the Chinese darknet markets provides request-to-buy mode. Users are no longer limited to browsing the displayed products but can make a request, which can be customised. The website structure of the Chinese darknet markets is simple but functional and helps locating products faster. Nevertheless, considering the profitability of the market itself, the English darknet markets are usually mixed with promotional products in all lists, and the promotional items are difficult to distinguish. On the other hand, in homepages, the English darknet markets use both pictures and text, while the Chinese darknet markets only have text. Physical items often need more pictures to display, while virtual items could use descriptive text only. This phenomenon reflects that different strategies apply to different types of popular products in different language darknet markets.

Product category. Drugs dominate the English darknet markets, while in the Chinese darknet markets the most popular category is personal data. Due to the convenience of express delivery in North America and Europe, and the different laws and regulations of each state or country, drug shipments are difficult to spot and stop. However, Chinese law enforcement is characterised by a heavy crackdown, deep inspection, severe sentencing, and heavy propaganda against drugs abuse. As of 2020, the number of drug abuse users in China has kept falling for three years in a row [27]. Regarding personal data, Chinese law enforcement agencies have been cracking down on telecom fraud in recent years. Most of them are related to the leakage of personal information. Due to the convenience of disseminating virtual items such as personal information, it is difficult to stop it. Pornography is the second-largest category in the Chinese darknet markets, which also contains child abuse. In the English darknet markets, they are clearly stated that child abuse is not allowed.

Market policy. English darknet markets restrict most high-risk products, such as arms, chemical weapons, child abuse, animal abuse, etc. There are no special restrictions on items in the Chinese darknet markets, but fraudulent behaviours with fake products in the market will be banned.

Payment method. Bitcoin is still the main currency in both English and Chinese darknet markets, and most English darknet markets also accept Monero for better privacy. In the Chinese darknet markets, users can even use fiat currency for small deposits.

Security mechanisms. The English darknet markets usually have stricter security measures than Chinese ones. More complex CAPTCHAs are used in the English darknet markets. The session time in the English darknet market usually has different time-window options, but it must be within a certain number of requests. Otherwise, users will be kicked out. However, since there is usually no limit on the number of requests in Chinese darknet markets, as long as the session is active, it will not be automatically logged out. In terms of account security, the Chinese darknet markets use the pay-to-activation method to control malicious registration, while the English darknet markets use the PGP public key.

2) Vendors: **Inactive days**. Vendors in the English darknet markets are more active than the Chinese darknet markets. The English darknet markets usually have a shorter life cycle. The three English darknet markets were established later than the Chinese Exchange Market. In the past, most English darknet markets were being shut down or scamming exits at the end, and then those market operators will usually change their identities and operate new markets. The new vendors in English darknet markets will remain active and establish their brand in dark web forums. Even if the market is closed, they can quickly sell in the new market because buyers usually follow good vendors. However, in Chinese darknet markets, even if the operators scam, they would not exit the market. They keep the operation as new vendors will not know because of lead of communication. Vendors in the Chinese darknet markets do not have to consider such feedbacks, so they also

spend less time in the market for such customer service. By comparing Figures 7 and 16, we can clearly find that some vendors are not active within a few months after posting their posts in the Chinese darknet markets.

Location. In the English darknet markets, the proportion of international vendors is greater because of the widespread use of English. Since some types of drugs are legal in some countries or regions, there are more vendors in non-English speaking countries in Europe. Because of the usages of language and jargon, we found that most of the vendors in the Chinese darknet markets are Chinese. However, Since mostly virtual products and pornography are sold, the vendor's real geographic location is difficult to measure.

Behaviour. Vendors in the English darknet markets pay more attention to building their own brands. Vendors in the English darknet market usually use their vendor profile or description section to promote themselves. Successful vendors claim and show their sales numbers and ratings in other well-known English darknet markets. They also explain the return policy and requirements, what will happen if the items are lost in transit. Vendors sometimes update new products or personal statuses. In the Chinese darknet markets, it is difficult for the vendor to do the same in the English darknet market because of the lack of functionality. However, we noticed that vendors in the Chinese darknet markets sometimes have their own language style, but it is still difficult to define the cross-market actors.

V. DISCUSSION

A. Insights

In comparison to their English counterpart, the ecosystem in the Chinese darknet markets remains relatively fragmentary, though innovation is high. The lack of any feedback and rating system likely contributes to make the vendors slightly less active. Chinese markets seem to serve mainly as a safer first point of contact rather than a full trading platform. Goods exchanges and price negotiations are likely to be carried out of the market, using other means of communication. We observed that both of the analysed Chinese darknet markets have a "private deal" section, allowing vendors to trade with specific target buyers. With the request-to-buy mode, buyers have more options than in English darknet markets. Chinese darknet markets may be improving and upgrading the functionality and security of their services by learning from the practices of English darknet markets. Moreover, as automated language translation becomes more and more accurate, markets in different languages can be accessed without the need for complex applications. That could become a new challenge for us. On the other hand, we can delve into how to use those technologies against crimes too, for example by creating a system that can detect cross-market illegal activities.

Chinese darknet markets have less stringent policies than English darknet markets. There are resources for child abuse, weapons and hire-to-harm in the Chinese darknet markets. The administrators usually do not care about the products sold, which is not the case in the English darknet markets. English

darknet market administrators have also began to focus on the quality of their products, for example by implementing the Product Quality and Harm Reduction programmes.

All markets suffer from reputation issues. On English dark web forums, we can see discussions or comments for each English darknet market. New markets will always appear, and most of the old markets will always gradually lose vendors and buyers for some reason. Some closed down, either because being seized or the operators performed exit scam. The Chinese darknet navigation website also displays comments from anonymous users on the Chinese darknet market. They usually complain about customer service and potential scamming activities. We may be able to explore such methods using specific indicators to predict scams before widely occurring. For example, in the Chinese Exchange Market, large-scale vendors are no longer active at the end of 2019.

Cross-market actors are active. We have seen the same vendors in all major English darknet markets. We speculate that international vendors are likely, especially for personal data, in both English and Chinese darknet markets. We found that the personal information data sold in markets contain leaked data from all over the world. Cross-market behaviour exists, and even on dark web forums, they use the vendor's identity to participate in discussions. It should be noted that this may also be one of the means to promote their own items. We also observed that they use other accounts to assume other identities. If we can track and link these accounts, we will be able to understand e-crime operations better.

B. Challenges

The main technical challenge we faced is the many restrictions these markets implement to stop or at least slow down automatic crawling and scraping of their websites. This is, obviously, a serious challenge for data collection. This is compounded with the instability of the Onion service, resulting in frequent but irregular interruptions to the data collection process. In addition, we must manually log in to each of our accounts before starting the crawler in order to get the cookies needed for the session. English markets are severely more restrictive in their anti-crawling measures, so we needed to maintain and operate multiple accounts simultaneously. In addition, markets operators frequently change the structure and the design of their websites, sometimes causing crawlers to fail. At times, markets operators update their security mechanisms without any notice, typically in ways that are damaging for bots but transparent for humans. For instance, the Cartel Marketplace updated their CAPTCHAs, and the Tea Horse Road also redacted the number of requests per session. In each of those cases, we must reconfigure our crawler. So data gathering becomes a continuous cat-and-mouse game, costly to maintain for large periods of time.

C. Limitations

Due to technical and time issues, there is an imbalance in the number of vendors between the English and the Chinese darknet markets. The more stringent crawling restrictions in the English darknet markets caused our crawler not being able to scrape all of the market content, resulting in a smaller amount of data being collected. In comparison, the Chinese darknet markets have less stringent restrictions, leading to more data points. Our dataset also contains a relatively short period of time in both English and Chinese darknet markets, so further work to expand our dataset would be worthwhile.

We have considered and dealt with bad data in our analysis, however, despite our best efforts, we still cannot guarantee the integrity of all figures such as prices and sales in any darknet market. As such, figures presented in this paper are based on our best estimation, which can and shall be improved in follow-up research.

VI. CONCLUSION

In conclusion, this paper has investigated and analysed the differences between darknet markets using English and Chinese as their main languages. The differences found are, at times, quite interesting and have a basis that is not only linguistic but also cultural. For this research, we collected data from five trending darknet markets, comprising three English and two Chinese darknet markets. Data collection was carried out for seven consecutive weeks.

English darknet markets generally seem to offer a more mature and complete ecosystem, with more active vendors than their Chinese counterparts. We found that the multiple differences between English and Chinese darknet markets are reflected across many aspects, including selling modes, product categories, market policies, payment methods, security mechanisms and vendors. In Chinese darknet markets, vendors are on average less active than in English darknet markets, but the demand and number of sales of personal data and pornography are relatively large. In English darknet markets, the main product sold are drugs. Moreover, the policies of Chinese darknet markets show that there are very few products banned, and the problem of child abuse material is extremely serious. In one of the Chinese darknet markets, fiat currency can be used, and the anti-crawling restrictions in both of the observed Chinese markets are easy to bypass.

Some interesting insights from our research is the existence of request-to-buy modes and some uncommon policy issues. We believe that these provide a way to gain comparative insights into darknet markets, and attract the attention of law enforcement agencies. In particular, this request-to-buy mode could be a good way to launch sting operations – where allowed by law. We hope that our study will provide a better understanding of darknet markets, particularly Chinese darknet markets. Future work can focus on vendor behaviour and cross-market operations in different language darknet markets. For instance, by using natural language processing techniques, we may be able to discover connections between vendors and identify potential cross-market international large-scale operators. Finally, the tracking of payment methods and profits is an additional interesting research path for the future.

REFERENCES

[1] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second-generation onion router," Naval Research Lab Washington DC, Tech. Rep., 2004.

[2] M. Reed, P. Syverson, and D. Goldschlag, "Anonymous connections and onion routing," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 4, pp. 482–494, 1998.

[3] U.S. Attorney's Office, "Ross ulbricht, the creator and owner of the silk road website, found guilty in manhattan federal court on all counts," 2015. [Online]. Available: https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/ross-ulbricht-the-creator-and-owner-of-the-silk-road-website-found-guilty-in-manhattan-federal-court-on-all-counts

[4] A. Hern, "Us seizes $1bn in bitcoin linked to silk road site," the Guardian, Tech. Rep., 2020.

[5] CNWest, "The "clean net" operation launched, six departments worked together to rectify harmful information on the internet," *CNWest*. [Online]. Available: http://news.cnwest.com/tianxia/a/2021/06/08/19728920.html

[6] 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, 2013, p. 213–224. [Online]. Available: https://doi.org/10.1145/2488388.2488408

[7] R. van Wegberg, S. Tajalizadehkhoob, K. Soska, U. Akyazi, C. H. Ganan, B. Klievink, N. Christin, and M. van Eeten, "Plug and prey? measuring the commoditization of cybercrime via online anonymous markets," in *27th USENIX Security Symposium (USENIX Security 18)*. Baltimore, MD: USENIX Association, Aug. 2018, pp. 1009–1026. [Online]. Available: https://www.usenix.org/conference/usenixsecurity18/presentation/van-wegberg

[8] A. V. Vu, J. Hughes, I. Pete, B. Collier, Y. T. Chua, I. Shumailov, and A. Hutchings, "Turning up the dial: The evolution of a cybercrime market through set-up, stable, and covid-19 eras," in *Proceedings of the ACM Internet Measurement Conference*, ser. IMC '20. New York, NY, USA: Association for Computing Machinery, 2020, p. 551–566. [Online]. Available: https://doi.org/10.1145/3419394.3423636

[9] K. Soska and N. Christin, "Measuring the longitudinal evolution of the online anonymous marketplace ecosystem," in *24th {USENIX} security symposium ({USENIX} security 15)*, 2015, pp. 33–48.

[10] A. Abbasi, W. Li, V. Benjamin, S. Hu, and H. Chen, "Descriptive analytics: Examining expert hackers in web forums," in *2014 IEEE Joint Intelligence and Security Informatics Conference*, 2014, pp. 56–63. [Online]. Available: https://ieeexplore.ieee.org/document/6975554

[11] V. Benjamin and H. Chen, "Securing cyberspace: Identifying key actors in hacker communities," in *2012 IEEE International Conference on Intelligence and Security Informatics*, 2012, pp. 24–29. [Online]. Available: https://ieeexplore.ieee.org/document/6283296

[12] B. Collier, R. Clayton, A. Hutchings, and D. Thomas, "Cybercrime is (often) boring: maintaining the infrastructure of cybercrime economies," 2020. [Online]. Available: https://www.repository.cam.ac.uk/handle/1810/306682

[13] P. H. Meland, Y. F. F. Bayoumy, and G. Sindre, "The ransomware-as-a-service economy within the darknet," *Computers & Security*, vol. 92, p. 101762, 2020.

[14] S. Pastrana, A. Hutchings, A. Caines, and P. Buttery, "Characterizing eve: Analysing cybercrime actors in a large underground forum," in *International symposium on research in attacks, intrusions, and defenses*. Springer, 2018, pp. 207–227. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-030-00470-5_10

[15] N. Christin, "An eu-focused analysis of drug supply on the alphabay marketplace," *EMCDDA commissioned paper*, 2017.

[16] M. Yip, C. Webber, and N. Shadbolt, "Trust among cybercriminals? carding forums, uncertainty and implications for policing," *Policing and Society*, vol. 23, no. 4, pp. 516–539, 2013. [Online]. Available: https://www.tandfonline.com/doi/abs/10.1080/10439463.2013.780227

[17] T. J. Holt, "Examining the forces shaping cybercrime markets online," *Social Science Computer Review*, vol. 31, no. 2, pp. 165–177, 2013. [Online]. Available: https://doi.org/10.1177/0894439312452998

[18] R. Bhalerao, M. Aliapoulios, I. Shumailov, S. Afroz, and D. McCoy, "Mapping the underground: Supervised discovery of cybercrime supply chains," in *2019 APWG Symposium on Electronic Crime Research (eCrime)*, 2019, pp. 1–16.

[19] G. Zhou and J. Zhuge, "Adapting to local conditions: Similarities and differences in anonymous online market between chinese and english speaking communities," in *International Conference on Digital Forensics and Cyber Crime*. Springer, 2020, pp. 164–181.

[20] Alsayra, "April 5, 2011-may 1, 2012. azsecure-data.org version." [Online]. Available: http://azsecure-data.org/get data/forums/alsayra.txt

[21] G. Branwen, N. Christin, D. Décary-Hétu, R. M. Andersen, StExo, E. Presidente, Anonymous, D. Lau, D. K. Sohhlz, V. Cakic, V. Buskirk, Whom, M. McKenna, and S. Goode, "Dark net market archives, 2011-2015," https://www.gwern.net/DNM-archives, July 2015, accessed: DATE. [Online]. Available: https://www.gwern.net/DNM-archives

[22] 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, 2018, p. 1845–1854. [Online]. Available: https://doi.org/10.1145/3178876.3186178

[23] I. Albery and M. Munafò, *Key concepts in health psychology*. Sage, 2008.

[24] D. Kouzis-Loukas, *Learning Scrapy*. Packt Publishing Ltd, 2016.

[25] J. Redman, "After empire's exit scam, darknet market patrons scramble to find alternatives," *bitcoin.com*. [Online]. Available: https://news.bitcoin.com/after-empires-exit-scam-darknet-market-patrons-scramble-to-find-alternatives/

[26] European Monitoring Centre for Drugs and Drug Addiction and Europol, "Drugs and the darknet: perspectives for enforcement, research and policy," 2017.

[27] Guangdong Drug Rehabilitation Administration, "China's drug situation 2020 report," Tech. Rep. [Online]. Available: http://gdjdj.gd.gov.cn/gkmlpt/content/3/3349/post_3349119.html#3346