A Qualitative Evaluation of Two Different Law Enforcement Approaches on Dark Net Markets

Cerys Bradley
Department of Security and Crime Science
University College London
London, UK
cerys.bradley.14@ucl.ac.uk

Gianluca Stringhini
Department of Electrical and Computer Engineering
Boston University
Boston, USA
gian@bu.edu

***Abstract*—This paper presents the results of a qualitative study on discussions about two major law enforcement interventions against Dark Net Market (DNM) users extracted from relevant Reddit forums. We assess the impact of Operation Hyperion and Operation Bayonet (combined with the closure of the site Hansa) by analyzing posts and comments made by users of two Reddit forums created for the discussion of Dark Net Markets. The operations are compared in terms of the size of the discussions, the consequences recorded, and the opinions shared by forum users. We find that Operation Bayonet generated a higher number of discussions on Reddit, and from the qualitative analysis of such discussions it appears that this operation also had a greater impact on the DNM ecosystem.**

***Index Terms*—cybercrime, policy, law enforcement, qualitative, drug markets, dark web**

I. Introduction

The Dark Web is the portion of the World Wide Web which is not indexed by search engines and is hosted on overlay networks such as Tor. Dark Net Markets (DNMs) are a particular kind of site found on the Dark Web which facilitated the trade in illegal goods and services, such as illicit drugs. The DNM Silk Road, which was created in 2011 and closed by the FBI in 2013, is often considered to be the first of the DNMs. Since the closure of Silk Road, the ecosystem has grown considerably with the creation of dozens more DNMs. Many of these DNMs have exceeded Silk Road in size and length of lifetime. Though the ecosystem has continued to evolve, law enforcement efforts to combat the space are a consistent threat. There have been several major efforts to close down DNMs and arrest their users. This paper is concerned with two of the most recent operations: Operation Hyperion and Operation Bayonet and the closure of the DNM Hansa.

Operation Hyperion took place in November 2016. It was a coordinated approach conducted by the Five Eyes Law Enforcement Group (FVEY) which involved approaching known and suspected buyers and vendors via letters, phone calls and in person. Some arrests were made but, in most instances, users were warned about the consequences of their alleged drug-related activity. Through this operation, the Swedish Police have claimed to have spoken to 3,000 suspects, the New Zealand Police have stated they approached 160, and the FBI 150 [18]. In addition, the Dutch Police created a Dark Net Site and publicly named DNM users under investigation [19].

Less than one year later, in July of 2017 the FBI closed the major DNM Alphabay in Operation Bayonet. They did not initially take responsibility for the site's closure in the hope that users would think it was an Exit Scam (when the administrators of a DNM close it, stealing any cryptocurrency held in escrow or user accounts) [20]. Whilst this operation was taking place, the Dutch Police had identified and seized the servers of another DNM, Hansa. Instead of taking Hansa offline, the Dutch Police continued to run the DNM as a large number of former Alphabay users tried to join the site increasing the number of transactions taking place. Hansa was closed on 20 July 2017, having been run as a honeypot for one month.

To date no academic research has formally evaluated the impact of either of these interventions and so it cannot be concluded if either innovative approach acted as a significant deterrence to users or otherwise reduced activity on the DNM ecosystem. This paper presents the findings of a study designed to qualitatively understand and compare the impacts of both approaches.

We conducted qualitative analysis on posts and comments extracted from two Reddit forums */r/DarkNetMarkets* and */r/dnmuk*. These now deleted subreddits were used by DNM users and non-users to discuss ecosystem wide issues including the operations that form the object of this study.

We find that the conversations surrounding Operations Bayonet and the closure of Hansa are much greater in number and list a greater number of impacts than those about Operation Hyperion. Further, the forum contributor opinions of both operations indicate that Operation Bayonet and the closure of Hansa had a greater impact. These findings shed greater light on cybercriminal behaviour and have implications for future cybercrime policy.

II. Related Work

Forum studies have been used to understand several aspects of the DNM ecosystem, including emerging drug trends [1], drug user experiences [1], [2], community values [3]–[5] and structure [6], and reactions to law enforcement interventions [7]. A range of approaches have also been utilised including quantitative analysis [1], [5]–[7] and qualitative analysis [2]–[5], [7]–[9], and active [1], [7] and passive engagement [2]–[5],

[8], [9]. The qualitative approaches to coding comments have included Grounded Theory [8], an adaptive coding system which is completely exhausted by the content [2], Corpus Assisted Discourse Studies (CADS) [4], imposing a pre-written taxonomy on content [5], [7], and Corpus Linguistics Assisted Discourse Analysis (CLADA) [9].

Cadevilla et al. [1] set up threads on a forum on the theme of medical advice and measured the community response (which was in the tens of thousands of visits) alongside dispensing advice. They argued that the threads were responded to positively [1]. In contrast, Bancroft and Reid (2016) explored existing community discussions on drug usage and safety. They collected 3,196 posts and comments from an active DNM forum in March, 2015. The content was hand coded around themes that included drug quality, dosage and usage and used to conclude that forums facilitate the dissemination of drug use safety and that contributors collaboratively assess the quality of drugs available on DNMs [2].

In addition to hand coding approaches, some researchers have utilised machine learning tools Working with the Agora forum collected by independent researcher Gwern Branwen, Luo [8] used TF-IDF and LDA analysis to organise posts and comments into definable, but potentially overlapping topics. The topics were defined by hand coding subsets of each allowing for a greater amount of content to be categorised. The 4 topics that emerged were invitation to treat (posts relating to business activities); risk management and social control; drug-related knowledge exchange; and community support [8]. Munskgaard et al. [3] used Unsupervised Topic Modelling to identify topics from posts and forums that had been reduced to bags of words. This research was also conducted on forums scraped by Gwern Branwen but looked at multiple forums. The purpose of this study was to understand the evolution of Libertarianism as understood by forum contributors.

Other research explored th econcept of Trust on DNMs. Lorenzo-Dus and Di Cristofaro [4] used the forums of Silk Road and Silk Road 2.0 from Branwen's dataset and the CADS approach to identify key words associated both with the term "trust" and with key figures in the ecosystem. They use their findings to argue that the way vendors are discussed is polarising, i.e. that vendors are either described in extreme positive or extreme negative terms, and that contributors both appear to trust the forum with personal information and use personal information to gain trust from other contributors [4].

Morselli et al. [5] conducted research on the forums of 10 DNMs to understand how conflicts are resolved. They developed a taxonomy of resolution strategies and of conflict causes and hand coded 200 discussion threads according to these taxonomies [5]. This enabled more quantitative measures of the distribution of different conflict and resolution types leading to the conclusion that the majority of conflicts were caused be transaction failures or scams and that ostracism, third-party mediation, tolerance, and avoidance were the most frequently used methods of resolution [5].

Rekvscna et al. [6], measured the structure of 26 forums using data scraped from live DNMs. Measurements such as the assortativity and clustering were taken and showed that the network exhibited high dissortative mixing (highly connected nodes connected to less connected nodes) making these forums different to, for example, social networks [6].

Two forum based studies have been used to measure the impact of law enforcement interventions on the ecosystem and both studies have focused on the closure of Silk Road. In [7], comments from Silk Road, Agora, and Evolution forums were obtained from active forums and hand coded according to content, contributor type, and sentiment. It was shown that, though contributors discussed continuing to trade on other DNMs, more experienced contributors were less likely to use Silk Road 2.0 and that comments coded as negative received less approval from other contributors [7].

When the same operation was evaluated in [9], the focus of the study was to understand how contributors felt about the escrow system used by Silk Road and Silk Road 2.0. CLADA was used to identify statistically significantly occurring collocates to the word "escrow" and assign sentiment to them [9]. The change in sentiment towards the escrow service was then measured before and after the closure of Silk Road and used to conclude that users were more positive towards the escrow system prior to Silk Road's closure.

Whilst forum data is able to shed light on the thought processes and opinions of contributors, it cannot be known how many forum contributors are also active on the ecosystem. Further, there is no way of demonstrating if the claims made on the forums are true. An alternative approach to measuring the impact of law enforcement operations is through quantitative analysis of the DNMs themselves. There have been multiple studies of this nature [7], [10]–[16].

These studies have considered the change in population [12]–[15], number of listings [12]–[15], [17], product prices [14], and volume of sales [14] often collected from scraped data [15] particularly scrapes collected by independent researcher Gwern Branwen [13], [14] though also through manual extraction [12]. For the most part, it has been concluded that the size of the ecosystem recovers after interventions [7], [10]–[14], [22]. In this paper we are the first to to evaluate specifically Operation Hyperion and Operation Bayonet and the closure of Hansa. Unlike other research that used dedicated DNM forums, we are also the first to utilise Reddit forums to understand DNM users.

III. Data

The data from this study was collected from two subreddits */r/darknetmarkets* and */r/dnmuk*. */r/darknetmarkets* was created in December 2015 and banned in March 2018 as it was deemed to be facilitating the sales of illegal goods and services. */r/dnmuk* was created in January 2016 and banned at the same time for the same reason.

Banned content is no longer accessible, however, Reddit user Stuck_In_the_Matrix has extensively scraped the contents of the site and made their repository available for research in 2015 [23]. Posts and comments can be accessed, separately,

from Google's online data analysis facilitator BigQuery [1] in monthly snapshots.

As Operation Hyperion took place in November 2016 and Operation Bayonet and the closure of Hansa in July 2017, we collected posts and comments from 1 September 2016 and 30 November 2017 (i.e. 3 months either side of the measurement period. This process returned 40,353 posts and 581,465 comments from the subreddit */r/darknetmarkets* and 18,890 posts and 285,791 comments from the subreddit */r/dnmuk*. For each comment and post, we collect the time at which it was posted, its textual content, and the user account under which the message was posted.

Because of the way the data had been stored the posts and comments needed to be aggregated by linking each comment's *parent_id* to a post *name*. Not every comment could be linked to a post and, in these instances, a dummy post was created. Additionally, the monthly snapshots were combined and duplicate posts and comments were removed.

After the aggregation process, the subreddit */r/darknetmarkets* contained 324,120 posts and 572,585 comments and the subreddit */r/dnmuk* contained 168,873 posts and 281,248 comments giving a total number of 492,993 posts and 853,833 comments across the dataset.

97% of the *parent_id*'s could not be matched with post names, implying that a large number of posts are missing from the dataset. However, by inspecting the comments, it was observed that many appeared to be direct replies to other comments (as they directly quoted another comment found in the dataset). It is therefore assumed that the *parent_id* on these comments matches with a value given to another comment which was not recorded in the dataset and so the number of missing posts is much lower.

The number of contributors to the subreddit was calculated by counting the number of usernames recorded in the dataset. Of the 347,844 unique contributors in the subreddit */r/darknetmarkets*, 69,858 contributors had the name '[deleted]'. This was assumed to represent when contributors had either deleted their account or been removed from the forum. To avoid conflating these contributors, each deleted contributor was given a separate user ID. Ultimately, this will overestimate the number of contributors as it is likely some accounts made multiple contributions before they were deleted. After this process, 618,493 contributors were found across both forums.

These estimates imply that contributors made, on average 0.797 posts and 1.38 comments. This could be because contributors interacted with the forum only a small number of times or that they made an effort to switch accounts between contributions.

To measure the connectivity of each forum, they were transformed into networks with contributors represented as nodes and edges drawn between two nodes when one had commented on the other's post. The density of the network representing */r/DarkNetMarkets* is $1.73 \cdot \exp(-5)$ and the density of the network representing */r/dnmuk* is $4.95 \cdot \exp(-5)$ implying that both networks are sparse. However, because of the presumed gaps in the dataset, these values are all likely to be underestimates.

To evaluate the incompleteness of each dataset we used the number of posts, comments, and users recorded as '[deleted]' or '[removed]' as a metric. In the dataset for */r/DarkNetMarkets*, 38% of the posts had been deleted, 10% of the comments and 17% of the contributor accounts. For */r/dnmuk* 26% of the posts found were deleted, 6% comments and 14% of the contributor accounts. Despite the high volume of presumed deleted material, there was still a sufficient amount of content to evaluate what had been discussed on each forum, even if it can not be concluded that this content represents the whole discussion on the forum.

To determine if these values were particularly high, perhaps due to contributors being more careful, given the nature of each subreddit's content, they were compared to the proportions of deleted content for a non-Dark Web related subreddit. The subreddit chosen was */r/Ebay* which was collected across the same measurement period.

The dataset created from this subreddit initially contained 20,558 posts and 88,076 comments. It was aggregated into a dataset with 54,606 posts and 87,264 comments. 759 (16%) of the posts were either of the form '[deleted]' or '[removed]' as were 6.4% of the comments and 10% of contributor accounts.

The proportions of deleted comments and users in each DNM subreddit were compared to the proportions in the subreddit */r/Ebay* using the Chi-Square test. The proportion of deleted posts was not compared due to the high proportion of dummy posts in each dataset. The Chi-Square statistics and p–values are given in Tab. I and show that the forum */r/DarkNetMarkets* has a higher proportion of deleted comments and contributors to a statistically significant level but */r/dnmuk* only has a higher proportion of deleted comments.

TABLE I
RESULTS OF CHI-SQUARE TESTS ON PROPORTIONS OF DELETED CONTENT

	Comments		**Contributors**	
	Test Statistic	*P–value*	*Test Statistic*	*P–value*
/r/DarkNetMarkets	0.0181	0.893	0.0729	0.787
/r/dnmuk	0.00115	0.973	0.0278	0.868

IV. METHODOLOGY

In order to evaluate the impact of each operation, we first needed to find the posts and comments made in discussions relevant to them. This section outlines how these posts and comments were identified, the methods used to extract themes and concepts from them, and how they were compartmentalised in order to compare impacts.

The relevancy of posts and comments was determined by two factors: their content and time stamp. This enabled both a quantitative and qualitative assessment of the discussions surrounding Operation Hyperion and Operation Bayonet and the Closure of Hansa.

[1] urlhttps://cloud.google.com/bigquery/

First, the number of posts and comments was measured over time to see if either intervention significantly increased the amount of content on the forum. To measure the significance of any fluctuations, a moving average was calculated with increases/decreases of 3 standard deviations from the mean considered to be anomalous.

Then posts and comments considered to be relevant to each operation were extracted. These were identified through key word searches. A separate list of keywords was created for each operation and was chosen in an attempt to identify all relevant posts/comments even if this resulted in some irrelevant content being collected.

For Operation Hyperion, the first set of posts and comments were collected in the week that the operation took place (22 – 28 October 2016). For Operation Bayonet and the closure of Hansa, posts and comments were drawn from two separate time periods, the first was from 1 – 12 July 2017. This time period covers from when Alphabay first went offline to the day before news stories about the alleged Alphabay administrator Alexandre Cazes' arrest were first shared on the forums. The second was from 13 – 27 July, which covers from the day information about law enforcement involvement in the closure of Alphabay came to light to a week after the closure of Hansa.

Initially each keyword list was searched for across all posts and comments. The datasets collated were then manually inspected to remove irrelevant posts and comments and identify additional relevant keywords and determine if the initial observation period needed to be increased leading to the expansion of the dataset through subsequent searches.

As this process was tailored to each operation, more details about the keywords and how the time windows were expanded are given in Section.V.

Key themes were extracted from the dataset using Grounded Theory. This is an iterative approach that involves reading content to identify concepts that are substantiated through rereading and additional data collection. The motivation is to firmly ground any concepts within the data itself, instead of searching for evidence of pre-considered ideas [21].

In practice, this process involved reading through each dataset once noting any concepts. These concepts were then aggregated into a list of themes which were reapplied to the dataset using Directed Content Analysis. As a result, each dataset was attributed its own list of themes and these were compared in order to determine how the different operations, and stages of operations, had affected the discussions on the forums.

V. Results

In this section, the findings from the qualitative analysis of each portion of the dataset are presented. Due to space constraints, the themes that emerged from each observation period can only be outlined. First we present the quantitative measurement of the size of the forums and their discussions. We then proceed illustrating the results of the qualitative analysis.

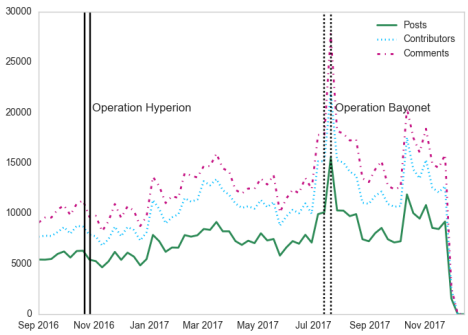

Fig. 1. Number of Contributors, Posts and Comments in the DNM threads over the measurement period

A. Quantitative Measurement

Fig. 1 shows the number of posts, comments and contributors on both DNM subreddits across the measurement period. Clearly, a there is a period of heightened activity in the week beginning 13 July 2017. This is the date that the FBI announce their involvement in the closure of Alphabay. In this week, the number of posts rises from 10,122 to 15,523, the number of comments rises from 17,829 to 27,803 and the number of contributors rises from 15,181 to 22,035.

The amount of activity was already higher than average (the average number of posts, comments and contributors per week is 4,780, 8,420 and 6,200 respectively). To measure if it is significant increase in activity, a moving average was employed. When the window of the moving average is 15 or above, the number of posts, comments, and contributors is more than 3 standard deviations from the mean. This is illustrated in Figs. 2, 3, 4.

A comparable increase in activity cannot be seen in the week of Operation Hyperion, nor in the weeks succeeding it. Indeed, in this week the number of posts, comments and contributors falls (from 6,296 to 5,411, 11,282 to 9,651, and 8,683 to 7,882 respectively) though this change is only measured to be, at most, 1 standard deviation from the mean.

This implies that the revelation that Alphabay was closed by law enforcement and the subsequent closure of Hansa garnered more discussion than Operation Hyperion. This disparity in impact is not only seen in the amount of content but also in the content itself.

B. Operation Hyperion

The keywords used to identify posts relevant to Operation Hyperion were words relating to law enforcement or the mechanisms of the operation (e.g. references to letters or arrests). They are listed in Fig.5. 'LL' and 'love letter' are colloquialisms which refer to a letter from law enforcement, most commonly informing the recipient their parcel has been seized.

There were 4,624 posts on the subreddit */r/DarkNetMarkets* and 729 on the subreddit */r/dnmuk* during the week of Op-

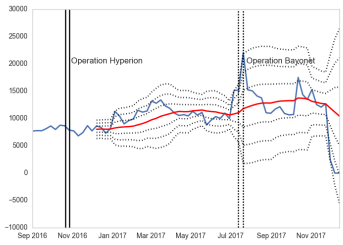

Fig. 2. Number of Contributors and Moving Average with 15 Week Window.

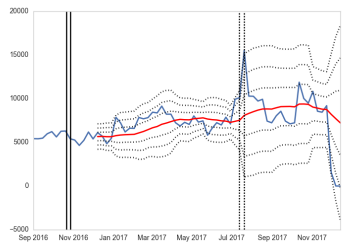

Fig. 3. Number of Posts and Moving Average with 15 Week Window.

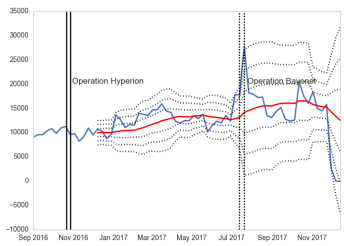

Fig. 4. Number of Comments and Moving Average with 15 Week Window.

‘arrest’, ‘love letter’, ‘ LL’, ‘a letter’, ‘police’, ‘nca’, ‘policeman’, ‘law enforcement’, ‘l.e.’, ‘ LE’, ‘fbi’, ‘operation’, ‘hyperion’, ‘confiscat’, ‘seiz’, ‘missing’

Fig. 5. Keywords used to identify relevant posts

eration Hyperion. 158 and 26 of those posts (respectively) contained or had a comment which contained, at least one keyword giving a total of 184 posts and 1,002 comments. Of these, 14 posts and 69 comments were deleted or removed from the subreddit.

Each post and comment was read to determine its relevancy. Contributions were considered relevant if they referred to a specific event that appeared to be taking place (i.e. not talking about law enforcement in general) or one of the tactics employed within the operation. Posts or comments that referred to letters had to explicitly state that the recipient was in some way under suspicion (as per the approach of Operation Hyperion) rather than discussing a generic customs letter. Only 8 posts were considered to be potentially relevant to Operation Hyperion.

This initial reading led to the removal of the words “confiscate”, “seiz” and “missing” from the set and “letter” by itself was added. In addition, the time window was extended by a month. This led to 896 posts being found in the subreddit */r/DarkNetMarkets* and 157 in */r/dnmuk*. Of these, 78 posts were confirmed as relevant.

Finally, to search through the rest of the data set, Operation Hyperion was searched by name (all posts containing the term “hyperion” were collected) adding a further 38 posts to the dataset which now contained 116 posts, the last of which was on 20 July 2017.

The following themes were identified in the posts and comments relevant to Operation Hyperion:

- **Description of the Operation:** posts and comments in this theme describe the nature and extent of Operation Hyperion. This was either in the form of sharing news articles about the operation or letters, visits, and phone calls that contributors received. Many of the personal experiences explained that law enforcement had information about their purchasing habits prior to 2014. Articles were shared from a variety of different sources including ice.gov, stuff.co.nz, motherboard and cyberscoop.com and, often, contributors would copy and paste the contents of an article directly into a post, instead of sharing a link. Individual instances that were described on the forum were rarely linked to Operation Hyperion or to each other. Additionally, this only occurred after official statements were released. The number of experiences shared that has been observed is far lower than the official figures given by official law enforcement statements.
  Potentially, many of the targets of Operation Hyperion did not realise they were part of an international operation and instead believed law enforcement was conducting a personal investigation. There is a chance, therefore, that more forum users reported their experience but these reports were not identified because they did not use the same language to describe what had happened. As many users reported that the information law enforcement was operating on was from purchases prior to 2014, some of the targets may have ceased their DNM related activities and so were no longer participants on the forum.
- **Speculation on How Operation Hyperion was Conducted:** when discussing the mechanisms of Operation Hyperion, contributors often speculated on how the evidence law enforcement claimed to have had been collected. The theories most popular theory was that law enforcement was utilising data collected in the closures of Silk Road and Silk Road 2.0. Some contributors felt that law enforcement were only able to use data that had been sent unencrypted through these sites where as others felt that they had been able to break the encryption schemes used to send messages (hence why they were only operating on this data 3 years later). A much less popular theory was that law enforcement had traced users using the Bitcoin blockchain. Prior to press releases about the operation, some contributors thought that law enforcement had identified a vendor who was using buyer addresses as the return address on their parcels.
- **Potential Consequences for Suspects:** as Operation Hyperion was unfolding it was linked by some contributors to a high seizure rate of packages sent from Canada to the UK. This was the dominant impact identified by users and led some to query if they should stop purchasing from Canada, or if Canadian vendors should stop selling to the UK. Despite this, the consequences appear to be

short lived with contributors explicitly arguing that it was safe for Canada and the UK to trade again from at least March 2017.

There was some additional speculation on what would happen to those users who had been approached by law enforcement. In the vast majority of instances, the conclusion was that there would be no further consequences and those that argued there would be consequences were not specific on what these might entail.

- **Advice Given to Suspects:** even though few consequences were discussed, a number of posts and comments either made or requested precautionary measures for the uses who had been targeted by Operation Hyperion. These were to move address or to stop ordering packages. However, many of the recommendations appear to have been intentionally hyperbolic, potentially to mock those concerned for their safety. It was recommended that users go to great lengths to destroy their computer or property or that they move to Belize (a joke from the series Breaking Bad). A common recommendation was also that users simply calmed down. These suggestions imply that many contributors felt there would be no serious consequences of the operation.
- **Opinions on Operation Hyperion:** in addition to discussing the operation itself, contributors shared their opinions on why it had happened, how it might affect the ecosystem in the future and if it was a legitimate action for law enforcement to take. Unsurprisingly, on the question of legitimacy, contributors felt that the operation was illegitimate. They argued that law enforcement should be more concerned by other threats, such as terrorism, and that attacking DNMs instead of legalising drugs was dangerous.

  Despite this, it was considered inevitable that law enforcement carry out some form of intervention against the ecosystem on a regular basis. Given this, some contributors felt that Operation Hyperion, when compared to previous operations, was quite mild. Some even felt that it was counter productive as the only consequence was to warn users who were being monitored.

  There were a few comments implying that contributors were intimidated by the operation but, for the most part, the operation seems to have been viewed as unsuccessful.

Based on the reading of the posts and comments found to be relevant to Operation Hyperion through these themes, the operation does not seem to have had a serious impact. Contributors appear to have taken Operation Hyperion as an indicator that law enforcement did not have the capacity to make arrests or similarly conduct a more impactful operation.

C. Operation Bayonet

The keywords used to identify relevant posts and comments to Operation Bayonet were "alphabay", "ab" (a common abbreviation for *Alphabay*), and "bayonet". To find posts and comments relevant to the closure of Hansa, the keyword "hansa" was used. As posts, and all the comments on that post, were recorded if any of the post's comments contained a keyword, this list was deemed to be sufficient as it was felt that all conversations about the closures of Alphabay and Hansa would mention either one of the sites.

Across the whole of July, there were 46,130 posts, 2,848 of which contained relevant keywords. This dataset was separated into two sets, one containing posts and comments prior to the FBI officially taking responsibility for the closure of Alphabay (on 13 July) an those during and after this event.

1) 1 – 12 July: Alphabay first went offline on 5 July, prior to this date no posts or comments indicated that contributors were worried the DNM was going to close. In the 8 days between Alphabay closing and official news of Alexandre Cazes' death reaching the forums, there were 708 posts and 2,716 comments containing keyword matches.

43% of comments were considered to be irrelevant, these covered topics such as vendor reviews, tumbling services, general queries about other DNMs, and a Fentanyl related death that had been connected to Alphabay.

For the remaining posts and comments, the following themes emerged:

- **Losses:** in at least 164 comments, contributors described how the closure of Alphabay had impacted them. They identified the following losses (given in order of frequency): losing money held in escrow, losing an order they paid for but was never shipped, losing the reputation they had earned on the DNM, and losing contact with a trading partner. The majority of comments on this theme were about losing money with some contributors claiming to have lost tens of thousands (of unspecified denomination). Additionally impacts identified included an increase in scams with DNM users impersonating Alphabay vendors or creating fake Alphabay sites in phishing attacks.

  Some contributors were concerned law enforcement had shut down Alphabay and so were worried that any data they had shared with the site was now known to law enforcement. These contributors were advised to change their passwords and, in a few extreme cases, get a lawyer.

  In nearly 10% of comments found on this theme, contributors claimed they had not lost anything or otherwise been affected, however it is unlikely that the true ratio of users who suffered losses and those who did not is the same as contributors who were impacted may be more likely to post on the forum for commiseration, sympathy, and to get advice.

  Often the contributors claiming to have suffered no losses stated this was because they had taken the necessary precautions and blamed those who had lost money on the fact they had kept any money in their account wallet.
- **Theories:** as, at this point, contributors were unsure what had happened to Alphabay, approximately a quarter of the discussion was speculation on why Alphabay had closed. The most popular theory, posed in nearly half the comments, was that Alphabay had closed in an exit scam, this was followed by the theory that it had been shut down

by law enforcement, then that it had closed temporarily for site maintenance or because it had been attacked. A few contributors suggested it had been closed by Russian Mafia (at the time, Alphabay was widely believed to be hosted in Russia and run by Russian carders).

The theories that argued Alphabay was closed permanently grew in popularity over time, where as the theory that the shut down was temporary diminished as time went on with no word from the administrators of the site.

Contributors also attempted to dispute others' theories. They argued against law enforcement involvement on the basis that no official statement had yet been released and that the DNM's security was too high. Contributors were sceptical that the DNM shut in an exit scam because withdrawals were not disabled in the days before the DNM went offline.

- **Permanent vs Temporary:** an extension of the theme of theories, contributors also speculated on whether or not the closure would be temporary or permanent. Comments were considered to demonstrate the contributor felt Alphabay was gone permanently if they explicitly stated it was, actively sought a replacement for the DNM or stated they felt it was more likely to be down permanently where as if the comment explicitly referred to Alphabay coming back online, discussed how they intended to use the site in the future or otherwise discussed Alphabay in the present tense, asked other contributors to stop claiming the DNM was down permanently or supported the site maintenance theory then the comment was coded as temporary.

  Marginally more comments implied that contributors thought the closure was temporary and these comments were more common at the start of the observation period but diminished over time.
- **To Trade or Not to Trade:** the final theme from this observation period was whether or not it was safe for users to continue trading on the ecosystem. Out of 132 comments in which this theme is directly referred to, just 2 indicated that the contributor would leave the ecosystem permanently and 7 indicated they would take a temporary break. They cited having bad luck with exit scams and no longer having access to the products they wanted as reasons for leaving.

  For the remaining comments on this theme, contributors discussed which DNM they should continue trading on with Hansa being the most recommended. Not only this, but the next most recommended DNM, Dream, received almost as many negative comments as it did positive where as Hansa was only explicitly disliked by 3 comments. Contributors who recommended Hansa predominantly did so because they felt its multisig facilitation made it safer. Other DNMs that were discussed were CGMC, DHL, RSClub, Traderoute, Valhalla, Wallstreet, and Zion.

2) 13 – 31 July: Using the same keywords, there were 2,140 posts and 8,421 comments in the time period 13 – 31 July 2017. Of these, 804 (10%) of the comments had been removed or deleted, 2,113 (25%) of the comments did not contain enough information to be labelled and 1,244 (15%) were determined to be not relevant.

The comments considered irrelevant covered 9 different topics: advertisements for products; bust and arrests that were not related to the operation; disputes between users that had not been caused by the operation; discussions of drug usage; general ecosystem queries; order queries; reviews; shitposting (jokes or intentionally misleading comments); and, technical queries that were not about improving OPSEC in the wake of Operation Bayonet.

In the remaining posts, the following 9 themes emerged:

- **Alphabay Admin:** on 13 July 2017, news outlets reported of the arrest and death of Alexandre Cazes, the alleged administrator of Alphabay under the names DeSnake and Alpha02. Cazes was arrested in Thailand and later reported to have committed suicide in custody. Posts and comments on this theme discuss Cazes as a person and speculate on the nature of his death.

  The contributors who discussed Cazes as an individual present a polarising view in which he was both perceived as an extremely talented programmer who made a great contribution to the ecosystem and a reckless, misogynist who got himself caught because of his lavish lifestyle and conspicuous spending.

  Many contributors did not believe that Cazes' death had been accurately reported, some thought he was still alive and in witness protection and others that he had been killed so that he wouldn't jeopardise the investigation. This high level of scepticism in mainstream news reporting demonstrates how forum participants can filter information in order to suit their own narrative.
- **The consequences of the operation:** this was one of the largest themes that emerged from the posts and comments. At least 9 different consequences were listed including the acquisition of data by law enforcement; accounts on other DNMs becoming compromised; users losing access to the ecosystem, money in their accounts, an order they had placed before the closures, and/or contact with a trading partner; a heightened number of scams and phishing sites; addiction and withdrawal related harms for drug users; and, impacts on related technologies such as a loss in the value of Bitcoin.

  After 13 July 2017, the proportion of contributors recording financial losses reduced (from over 60% to 13%) and many more contributors expressed concern for law enforcement gaining access to their data. Some comments explicitly expressed the sentiment that the seizure of data was worse than the seizure of cryptocurrencies. Contributors were concerned that the acquisition of data would lead to arrests, however the comments describing explicit consequences were in the minority. Even though less financial losses reported in this time period, some

contributors described how they had lost funds twice because of both site closures, demonstrating how the consequences of this intervention were compounded.

In addition to sharing the impacts of the operation, comments on this theme discussed who specifically would experience these impacts. In general, contributors were convinced that law enforcement would be targeting either vendors or buyers buying for resale and that buyers purchasing for personal use would be unaffected. Though, a small minority were worried that, on this occasion, law enforcement would make arrests of these small time buyers as a warning. Additionally, many contributors argued that the only users vulnerable to being arrested were those who failed to properly protect themselves by encrypting their information.

Ultimately, even though many impacts were described, the impression given by contributors assessing the severity of the operation was that it would be temporary and surmountable. This was, in part, because of the strong narrative arguing that only those who had made mistakes would be affected.

- **Whether or not users would continue trading:** this theme contained posts and comments in which contributors either explicitly stated that they would continue or stop trading or implied this (for example, by discussing where they would set up their next account).

  In most (approximately 85%) of the comments in which contributors explicitly stated if they were going to stop or continue trading in light of the site closures, contributors claimed they would continue to trade. Though, often, this decision was caveated for example by contributors only prepared to make small purchases from trusted vendors through direct deals, rather than on a DNM.
- **Hansa:** Hansa was not closed until 20 July 2017, 7 days into this observation period. During that time, new account creation on the site was suspended and reopened and the sale of Fentanyl was banned.

  Many users felt that Hansa was the best available DNM now that Alphabay was closed due to its good interface and the fact that it was believed Hansa's multisig feature would offer greater protection against an exit scam. These comments, and the fact that so many users tried to join the site causing account creation to be suspended, indicate that no one was expecting its closure. There were, however, a few comments on the day of Hansa's closure in which contributors complained of issues when trying to withdraw money from the site. Immediately after Alphabay's closure, contributors argued it had not closed in an exit scam because there were no problems with withdrawals and that this is an obvious indicator a site is about to close. Despite this, no of the contributors predicted that Hansa would close in these discussions.

  The other major discussion concerning Hansa was the ban on Fentanyl which occurred on 18 July. This issue appears to have split the community with half of the comments arguing that the ban was contrary to the Libertarian principles of the ecosystem and that it was hypocritical to ban only this drug. However, as many comments argued that Fentanyl was not too only dangerous but also attracting more attention from law enforcement and that, if they banned it, Hansa was less likely to be closed.
- **Opinions:** this theme contains all comments and posts in which contributors shared their opinions about Operation Bayonet and the closure of Hansa, i.e. if they thought intervention was illegitimate and if they thought it was successful.

  Unsurprisingly, nearly all the contributors who commented on the legitimacy of the intervention felt that it was illegitimate. In particular, contributors thought it was hypocritical for law enforcement to have run Hansa as a honeypot as this facilitated the sale of drugs. However, more generally, contributors thought that any action to attack the ecosystem made it more dangerous for drug users to acquire and consume drugs and was therefore illegitimate.

  To evaluate the success of the site closures, contributors discussed if they would stop people from using the ecosystem. Though most of the emotions used in conjunction with the operations were negative (for instance describing them as "irritating" or "depressing"), most explicit evaluations of the operations argued that they would ultimately be unsuccessful. It was argued that law enforcement were exaggerating the results of the closures, particularly when it came to arrests, and that law enforcement would now be so swamped with data they would not actually be able to conduct investigations. Some contributors used the history of the ecosystem to argue that it always regrew after similar operations.

  Despite this some contributors (in approximately 19% of comments) felt that the operations had been successful, that they had affected many users and that these site closures had been the most devastating to date. Many of these comments were met with accusations of Fear, Uncertainty and Doubt (FUD) a concept within the forums used to accuse others of creating unnecessary panic.
- **OPSEC:** posts and comments on this theme discussed how users could improve OPSEC, either to protect themselves from the consequences of these site closures or against future operations. These recommendations included (in order of number of recommendations) cleaning house, taking a break from trading, using PGP to encrypt any messages and improving online security more generally for example by switching to I2P services and using a more secure cryptocurrency instead of Bitcoin (Monero was most frequently recommended). There was also a discussion about the security properties of multisig.

  As with the discussions after the closure of Alphabay, and after the closure of Hansa, there was an emphasis on how individuals could improve their security practices. However, perhaps because of the multiple site closure, there was also a discussion about how individual DNMs could improve security as well. As part of this discus-

sion, contributors argued that DNMs should no longer provide an auto-encryption feature as this was felt to have encouraged laziness and allowed law enforcement to collect more information on users. Contributors also wanted future DNMs to be decentralised to make them harder to close down and facilitate multisig transactions to minimise the financial impact of closures.

Not all contributors expressed positive emotions towards multisig transactions. At this stage, it was still unclear if users would be able to recover any money being held in multisig wallets for transactions and so some contributors argued that the technology had not protected users in the closure of Hansa. It was also theorised that law enforcement had used the multisig mechanism to infect vendors with malware. However, defenders of multisig transactions argued that Hansa had simply not implemented it properly and future implementations would be more secure.

- **Other DNMs:** after Hansa closed there was an increase in the discussion of other DNMs. The alternative DNMs were Dream (the most discussed), Traderoute (the next most discussed but by a considerable amount), DHL, Greenroad, Sourcery, TMG, Tochka, Valhalla, Wallstreet and Zion. Contributors discussed which DNMs were safe to use as many were concerned that another DNM would soon be closed and revealed to be a honeypot, as well as which DNMs were good trading platforms.

  Contributors struggled to choose a suitable alternative as Dream, which was the largest, was considered unreliable and shut down several times during the observation period making contributors concerned it would soon exit scam. However, the other DNMs were considered to have too few vendors and products available.

  A further complication was that contributors were concerned about more law enforcement activity. It was argued that, because Hansa was the most recommended alternative to Alphabay the movement of former Alphabay users to Hansa was orchestrated by law enforcement and, therefore, the most recommended DNM after Hansa closed was also a honeypot. This appears to have made it difficult for users to settle on a DNM to recommend.
- **Other operations:** contributors brought knowledge of past law enforcement interventions, specifically of Operations Onymous, Hyperion, and Titanium (Tools for the Investigation of Transactions in Underground Markets), when discussing this intervention. These operations are only mentioned in this time window, i.e. after law enforcement involvement is confirmed.

  Operation Hyperion was used to diminish any consequences of data collection by contributors who said that, the only consequence of that operation had been warnings several years after the data had been collected.

  Operation Onymous was used by contributors to make the point that these sorts of law enforcement operations happen periodically and to share advice on how to survive them.
- **Theories:** the final theme was one in which contributors shared theories on how they felt law enforcement had managed to seize and close both DNMs. This included the sharing of official statements and alternative theories posed by contributors.

  For both closure of Alphabay and Hansa, the relevant law enforcement agency officially claimed they were able to locate the servers of the DNM and its administrators through an admin error. In the case of Alphabay, it was claimed that Alexandre Cazes' e-mail address had been leaked by the software used to create the forum and, for Hansa, law enforcement claimed they identified the admin of the site when investigating a surface web e-book site. Some contributors, however, felt that these were false explanations, or "parallel reconstruction", i.e. that law enforcement had identified the locations of the servers through other means and then been able to construct these plausible alternative theories. The fact that two DNMs had been taken offline led some contributors to worry that they had been found because of a vulnerability in Tor however, theories in which individual admin had revealed themselves through bad OPSEC were more popular.

VI. Discussion

From this qualitative assessment of both Operation Hyperion and Operation Bayonet and the closure of Hansa, we find that not only was there a larger discussion surrounding the later two actions but that the impacts described by contributors was also greater. Contributors seemed more concerned by the tangible effects of Operation Bayonet and the closure of Hansa (such as losing money), were more likely to say they wanted to either take a break from the ecosystem or stop trading entirely, and spent more time discussing how and why the operation had taken place.

When comparing the closure of Alphabay before and after information about the involvement of law enforcement came to light, we see that a higher proportion of contributors claim they will stop trading after they know about the law enforcement involvement and after Hansa also closes. However, these contributors are still in the minority. The types of impacts described also changes with most contributors being concerned about financial losses in the first observation period but more being concerned about the law enforcement acquirement of data in the second. This may be because less money was lost by Hansa users, because of the multisig system (though at the time most contributors did not know if they could recover any money involved in trade when the DNM closed) or because contributors saw the potential for arrest as a greater threat. This hypothesis is both supported by contributors who explicitly argue the seizure of data is worse than the seizure of cryptocurrency and disputed by contributors who point to Operation Hyperion as an example of how law enforcement cannot act effectively on data they collect.

A consistent narrative across all measurement periods is that the contributors who were either greatly impacted or seen as most likely to be impacted were those who were

perceived as not taking sufficient precautions, e.g. they stored cryptocurrency on the site or failed to use PGP encryption. Similarly, when speculating on how different operations had taken place, the most popular theories involved individual admin mistakes, as opposed to law enforcement exploiting vulnerabilities in specific technologies. This could be because some of these theories are supported by official statements but could also represent the idea that contributors feel more secure when they believe their security is within their control, which would not be the case if the tools they use to protect themselves are vulnerable.

Finally, posts and comments found within this dataset demonstrate that contributors expect law enforcement operations to take place. Whilst there are some contributions which imply Operation Bayonet and the closure of Hansa made contributors unwilling to trade on the ecosystem, at least in the short term, there were also many comments which implied contributors were confident in the ecosystem's ability to recover.

We use these findings to conclude that it is likely Operation Bayonet and the closure of Hansa had a greater impact on the DNM ecosystem than Operation Hyperion. And that, if this was the case, it is because the effects of the former were more immediate and created more uncertainty.

A. Limitations

The findings of this study are limited both by the datasets employed and the methodology used to interpret them. The datasets used for this research are incomplete both in the sense that some posts and comments are known to be deleted and others are thought to have not been collected, but also because key information was not collected on the data. This information includes the title of posts and the ability to link comments that directly reply to others. As such, the context is missing for some comments.

This has implications for the external validity of quantitative analysis. Different approaches for assigning user ID's to deleted user accounts will lead to different conclusions on the number of users in the dataset. However, from an internal perspective, a consistent approach was employed that allows for approximate comparisons of the population size over time. Similarly, the statistics produced on the graph (such as density, etc.) are a result of specific choices that had to made when assigning ownership to posts and comments. Different choices would likely result in different statistics and so they are presented in this paper as approximations to give context to the qualitative analysis.

Additionally, the approach taken to identify relevant posts and comments may not have been exhaustive and so it cannot be guaranteed that all the discussions of each operation have been read. The choice to include all posts and comments from a thread if at least one post or comment contains a keyword reduces the chances of this. However, discussions of Operation Bayonet and the closure of Hansa were easier to identify. Therefore a different approach to sourcing discussions from Operation Hyperion could lead to different conclusions when comparing the impacts of the operations.

As this analysis has been conducted on Reddit forums, it is not known if the contributors to the forums are actual users of the DNM ecosystem. Further, it has been assumed that each contributor represents an individual but this might be the case. Finally, this study cannot confirm if the comments made in the forum are truthful. As such, the findings in this study may be an exaggeration of the impacts of each operation. Potentially, a quantitative analysis of the actual ecosystem population during both observation periods could help to validate these results.

VII. Conclusion

This paper reports the results of a qualitative study on posts and comments from two DNM related subreddits. Grounded Theory was used to understand themes and topics within posts and comments found to be relevant to Operation Hyperion and Operation Bayonet and the closure of Hansa. It is shown that Operation Bayonet resulted in more consequences for users being reported and that the use of Hansa as a honeypot caused serious immediate concern for the contributors who worried they had given data to the site.

References

[1] F. Caudevilla, The emergence of deep web marketplaces: a health perspective. The internet and drug markets.(European Monitoring Centre for Drugs and Drug Addiction: Insights 21), pp.69-75 (2016).

[2] A. Bancroft and P. S. Reid, Concepts of illicit drug quality among darknet market users: Purity, embodied experience, craft and chemical knowledge. International Journal of Drug Policy, 35, pp.42-49 (2016).

[3] R. Munksgaard and J. Demant, Mixing politics and crime – the prevalence and decline of political discourse on the cryptomarket. International Journal of Drug Policy 35 pp.77-83 (2016).

[4] N. Lorenzo-Dus and M. Di Cristofaro, I know this whole market is based on the trust you put in me and I don't take that lightly: Trust, community and discourse in crypto–drug markets. Discourse & Communication 12, no. 6 pp.608-626 (2018).

[5] C. Morselli, D. Décary–Hétu, M. Paquet–Clouston, and J. Aldridge, Conflict management in illicit drug cryptomarkets. International Criminal Justice Review 27, no. 4 pp.237-254 (2017).

[6] T. Rekšņa, Complex network analysis of Darknet black market forum structure. Master's thesis (2017).

[7] W. Lacson and B Jones, The 21st Century Darknet market: lessons from the fall of silk road. International Journal of Cyber Criminology 10, no.1 (2016).

[8] Q. Luo, An exploratory investigation into the darknet marketplace discussion forum Agora. Master's thesis (2017). unpublished.

[9] M. Horton-Eddison and M. Di Cristofaro, Hard interventions and innovation in crypto-drug markets: the ESCROW example. Policy Brief 11 (2017).

[10] K. Soska and N. Christin, Measuring the longitudinal evolution of the online anonymous marketplace ecosystem. In 24th USENIX Security Symposium (USENIX Security 15), pp.33-48 (2015).

[11] J. Aldridge and D. Décary–Hétu, A response to Dolliver's "Evaluating drug trafficking on the Tor Network: Silk Road 2, the sequel". International Journal of Drug Policy 26, no. 11 pp.1124-1125 (2015).

[12] J. Van Buskirk, A. Roxburgh, S. Naicker, and L. Burns, A response to Dolliver's "Evaluating drug trafficking on the Tor network". The International journal on drug policy 26, no. 11 pp.1126 (2015).

[13] R. Munksgaard, J. Demant and G. Branwen, A replication and methodological critique of the study "Evaluating drug trafficking on the Tor Network". International Journal of Drug Policy 35 pp.92-96 (2016).

[14] D. Décary–Hétu and L. Giommoni, "Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous. Crime, Law and Social Change 67, no. 1 pp.55-75 (2017).

[15] D. S. Dolliver, Evaluating drug trafficking on the Tor Network: Silk Road 2, the sequel. International Journal of Drug Policy 26, no. 11 pp.1113-1123 (2015).

[16] D. S. Dolliver, A rejoinder to authors: data collection on Tor. International Journal of Drug Policy 26, no. 11 pp.1128-1129 (2015).

[17] V. Bhaskar, R. Linacre and S. Machin, The economic functioning of online drugs markets. Journal of Economic Behavior & Organization (2017).

[18] Drugs Forum User 5–HT2A, 'Operation Hyperion' targets suspected Dark Web users around the world. Retrieved from https://drugs-forum.com/ams/operation-hyperion-targets-suspected-dark-web-users-around-the-world.26503/ (2016).

[19] E. Harfenist and M. Turgeman, Dutch police open Dark Net site to spook vendors and buyers. Retrieved from http://www.vocativ.com/372640/dutch-police-open-dark-net-site-to-spook-vendors-and-buyers/ (2016).

[20] Europol, Massive blow to criminal Dark Web activities after globally coordinated operation. Retrieved from https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation (2017).

[21] Grounded Theories Ltd, Grounded Theory getting started. Retrieved from http://www.groundedtheoryonline.com/getting-started/ (2019).

[22] J. Van Buskirk, A. Roxburgh, M. Farrell and L. Burns, The closure of the Silk Road: what has this meant for online drug trading?. Addiction 109, no. 4 pp.517-518 (2014).

[23] Reddit User Stuck_In_the_Matrix, I have every publicly available Reddit comment for research. 1.7 billion comments 250 GB compressed. Any interest in this?. Retrieved from https://www.reddit.com/r/datasets/comments/3bxlg7/i_have_every_publicly_available_reddit_comment/ (2015).