Dishing the Deets: How dark-web users teach each other about international drug shipments

Reagan C. Smith, Richard Frank
Simon Fraser University, School of Criminology
Burnaby, Canada
{reagans, rfrank}@sfu.ca

Abstract

International trafficking of drugs enabled by the dark-web is still a problem despite the increase in take-down actions. Even though the transaction takes place digitally, the national postal systems are the ones being exploited and used for delivery. Users of the dark-web readily share information on forums, cryptomarkets, and feedback pages to maximize their safety and success while conducting these drug transactions. Using data collected from forums, vendor profiles, and feedback pages, this study provides an evidence that the knowledge being shared on the dark-web is rich data law enforcement and governments need to use as intelligence. Users discuss all aspect of the delivery process, including proper addressing, stealth packaging, and risks associated with taking delivery of the package. Based on these findings, policy recommendations are made to guide the implementation of techniques to counter the rise of dark-web-enabled drug shipments in the fight against drugs and cryptomarkets.

1. Introduction

There exists on the Internet an anonymous and heavily encrypted sub-network, commonly referred to as the dark-web, enabled through the Tor software. Although the Tor network was designed to hide the routing information of its users from prying eyes and in the process anonymize its users, it has also allowed websites to be placed within this anonymous network. Malicious users have exploited this capability by setting up marketplaces within the dark-web; as these marketplaces are within an encrypted network they are commonly referred to as *cryptomarkets*. The creation of *The Farmer's Market* and *The Drug Store* in 2009 was the first unofficial documentation of dark-web markets [13]. Silk Road, operating between 2011 and 2013 before it was shut down by the FBI [12] enabled vendor revenue of around $1.2 million USD per a month [8][27] on illicit drugs, fraudulent identification papers, and credit card information. Much of this product was delivered through the traditional postal service.

In the United States, only 36% of inbound international mail is provided with electronic information about the importer and exporter [19]. The failure to collect information on these key actors allows malicious actors to exploit the postal system and increases the complexity of targeting efforts by customs and border patrol officers. The exploitation of the postal system to traffic drugs has proven to be a successful channel for cryptomarket vendors to ship products to buyers. Combined with the anonymity of the dark-web, law enforcement is struggling to catch up with the ever-complex techniques used by vendors and buyers to avoid law enforcement detection [1][15][21].

The dark-web, specifically the forums contained within it, vendor profiles, and feedback pages found on most cryptomarkets, not only allows for buyers and sellers to transact, but also for individuals to gather knowledge on techniques of law enforcement avoidance and educate themselves on the safest shipping methods available to them. Troubled by the influx in imported international mail and declining resources, law enforcement and government officials are only now grasping to catch up to the techniques vendors and buyers have implemented to get the products safely from one to the other [15][19]. The 2017 Global Drug Survey reports that of 5,565 American respondents, 25.5% respondents reported having bought drugs from the dark-web. To add to this, 25.3% of 3,118 UK respondents and 7.1% of 3,155 Canadian respondents also reported buying drugs from the dark-web [29].

Knowledge found on the dark-web ranges from packaging techniques and address formats to risks associated with various counties, controlled delivery protocols, and tips on customs and border patrol detection techniques and technology [1][21][10][25]. It's also argued that the live feed of knowledge being shared allows vendors and buyers to "gauge constantly changing risks" which in turn is "steadily eroding the long-term knowledge advantage" law enforcement had before the dark-web was popular [15]. The research in this paper will provide evidence that knowledge on

URI: https://hdl.handle.net/10125/64319
978-0-9981331-3-3

techniques to traffic drugs internationally without law enforcement disruption is not only commonly found but also a gap in intelligence that law enforcement should utilize. Recommendations will be made on approaches law enforcement should make towards the dark-web and why "knowledge research on the web should lead to strategies to disrupt the physical side" of drug trafficking [6].

2. Literature Review

2.1. Cryptomarkets

Cryptomarkets are online markets on the dark-web that can only be accessed through the anonymized browsing service The Onion Router [TOR] and use anonymous currencies (eg. Bitcoin, Monero) to complete transactions [15][2][21]. Like Amazon, eBay, or Craigslist, vendor success is levied on user feedback; feedback details product quality and quantity, stealth levels, speed, and overall transaction experience [2][6]. These markets allow vendors and buyers to stretch their business and drug habits across time and "create a global network of offenders"– all while being anonymous [2].

Compared to traditional "open" markets, their anonymity places them in a hybrid "open closed" category – open in plain sight for the public and law enforcement to see, yet identities and geographic locations are closed for viewing [2][1]. Through this anonymity, they are revolutionizing the way illicit drugs are being bought and sold. Surveys of users on the dark-web show most source their drugs only online as opposed to the streets. Reasons include: higher product quality, anonymity, convenience, and decreased risk [5].

Cryptomarkets allows users to search for specific products while vendors can market their business platform on individual vendor profiles (see Figures 1 and 2). The products being sold range from licit goods such as e-books and clothing to more nefarious goods like weapons and firearms, stolen credit data, computer hacking tools, and illegal narcotics [21]. Research shows most products found on cryptomarkets are illicit goods, with narcotics at the top of the list [15][21].

The marketplace that set the standard for cryptomarkets was Silk Road (SR), which operated from 2011 to 2013. Extensive research from crawling SR after the shutdown by the FBI shows that SR offered "220 distinct categories from digital goods to narcotics and prescriptions." The void left after the SR shutdown in 2013 allowed new marketplaces to quickly emerge [2]. Operation Onymous in 2014 saw a joint effort by the US and European countries take down over "410 hidden services" including top markets. The result of the "largest law enforcement action to date against websites operating on the Tor network" was a demand for an increase in anonymity and security on the dark-web by users [26]. To add to this, in 2015, the cryptomarkets *Evolution* went offline as the result of a speculated "exit scam". The marketplace operators shut down the platform and left with an estimated $12 million USD in Bitcoin from escrow transactions and vendor profits. As a platform built on trust between administrators, vendors, and buyers, the dark-web population lost confidence in cryptomarkets because of this event [11].

Until their shutdown by law enforcement officials in July 2017, AlphaBay and Hansa rose to become the largest and most popular cryptomarkets. The increase in opioid overdoses within the US, partially from dark-web fentanyl, saw AlphaBay under extreme scrutiny and surveillance from law enforcement and government officials. Although Hansa took the deliberate step of banning the sale of fentanyl and fentanyl analogues within their market, Dutch police took over the website and arrested the operators [18].

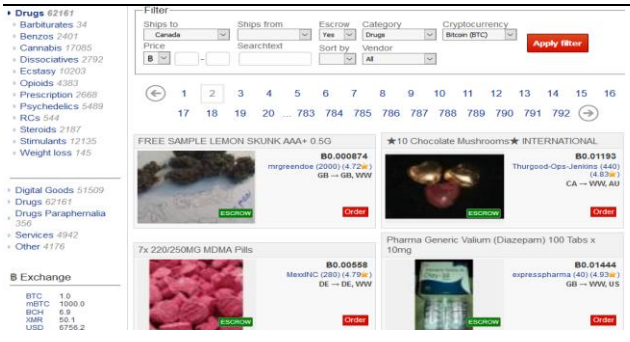

Figure 1. Dream Market drugs page. A page within the drugs section advertising a variety of drugs with the filters: "Ships to Canada", BTC, and "escrow".

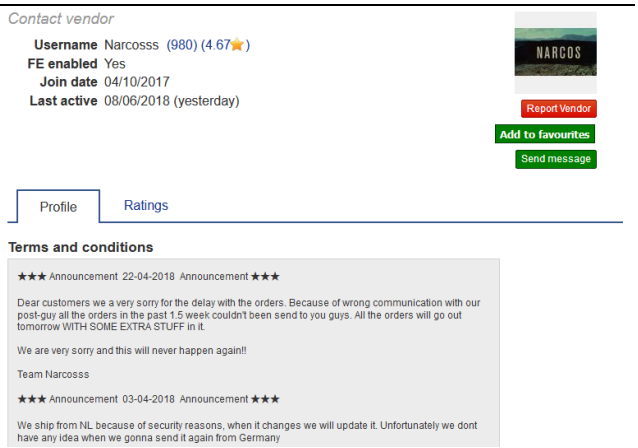

Figure 2. Vendor's profile. Vendor's profiles detail their reputation, activity history, and business platform for potential buyers to assess when deciding on a vendor.

2.2. The Postal System

Currently law enforcement, policies, and legislation are in place to ensure no threats are imported into a country, and customs and border patrol officers are the first line of defense towards illegal contraband, threats, and illicit goods being imported. It's also argued that the quantity of drugs passing through borders via the postal system is impossible to estimate, but the number of positive customer reviews on cryptomarket feedback forums attest the number being high [15].

The US Senate recently held a hearing to detail a study conducted by the Committee on Homeland Security and Governmental Affairs on the US Postal System (USPS) being exploited for the use of trafficking narcotics from the dark-web [19]. The pilot project, conducted by Customs and Border Patrol (CBP), USPS and the US Department of State, had the goal to investigate "measures used to prevent illicit fentanyl from entering the US" [19]. It was concluded that the biggest issue preventing the CBP officers and USPS postal inspectors from targeting narcotics more efficiently is the absence of automated electronic data (AED); AED was only provided for 36% of packages entering the US. Statistics show between 2013 and 2017 the quantity of inbound mail increased 237% - a growth not met with additional resources. In addition, the project found that there is a lack of cooperation and transparency between agency goals [19]. These results show evidence that the postal system is being exploited and more resources are needed towards fixing it.

2.3. Illicit drug shipping strategies

Online forums on the dark-web give buyers and vendors a "library on effective concealment and counter-interdiction techniques" [15]. Categories help individuals sort through the masses of topics quickly and efficiently. Topics regarding drugs on dark-web forums include: harm reduction, vendor reviews, paranoia stories, product sourcing, stealth techniques, risk countries, and general comments outlining personal experiences on the dark-web and cryptomarkets. Although it seems counter-intuitive for users to discuss details which would reveal to law enforcement the packaging secrets used by users to ship illicit drugs, and thus increase the chances of detection, there are regardless conversations which contain these details. Perhaps those users, like elite hackers, are motivated not entirely by profit, but by increasing their reputation within the forum. The higher the reputation, the more trust, the more business they can do. Alternatively, the individuals sharing this knowledge might not be sellers themselves, but administrators of the forum who are sharing this information to facilitate the marketplace.

Before being taken down in 2018, the subreddit r/darknetmarkets was one of the largest resources for dark-web conversations and links [3]. A thread on Reddit outlined specific techniques and details on avoiding law enforcement using "safe shipping". Details on packaging outlined red flags customs and border officers are known to look for: no return address, poor packaging, uneven weight distribution, drug source countries, person to person parcels, and excessive postage. In addition, the thread dove into the technology and investigation techniques border and customs officers use to target mail [10]. It's also believed that "there is an abundance of intelligence that can be viewed by law enforcement within these forums, but it is not being used in an effective manner" [1].

Unique and specific language is used on the forums to convey packaging techniques and behaviour to avoid law enforcement infiltration. In the context of this paper, the term "stealth" refers to the level of detail put into the packaging and tactics of a successful shipment. Researchers have carried out transactions on cryptomarkets and documented the packaging techniques [21]. The conclusion was drawn that the online description of packaging techniques matched the product they received – heat sealed bags, padded envelopes, printed labels, and a small baggie of the product [21]. These techniques are consistent with additional research on profiling parcels containing drugs [1][15][10].

2.4. Research Aim

The main aim of this study is to determine the extent of knowledge buyers and vendors of the dark-web are sharing. This will be determined through the collection of comments in three forms: customer feedback, forum comments, and vendor profiles. Through a qualitative assessment of these three categories, the aim is to find content concerning international drug trafficking which will allow comments specific to shared knowledge on evading law enforcement to emerge. Little research has been done on the area of using the dark-web as a knowledge network on how to evade law enforcement when trafficking drugs internationally. This study will help better understand how buyers and vendors of drugs on the dark-web are gaining knowledge on trafficking drugs through the postal system. It is hypothesized that enough knowledge will be found to understand the before, during, and after process of shipping drugs.

3. Methodology

Data collected for this research was obtained from two forums and one cryptomarket between the period of November 2017 and April 2018. These platforms were

accessed through the anonymized browser Tor. Due to the timeframe of the research, a purposive sampling was used to capture content specifically detailing techniques on how to ship drugs internationally. Aldridge and Askew's (2017) research provided a starting list of keywords to identify discussions and comments that should be picked out for analysis [1]. These keywords, along with an ensemble of additional original keywords, included: stealth, packaging, shipping, parcel, customs, borders, and mail. The additional words chosen were commonly found words and themes during literature reviews of the dark-web. The final list of keywords was used as a guide, with others added to the list if deemed important. Data was archived, and analysis was performed using Microsoft Excel and NVivo. Excel Pivot tables were used to allow any patterns and trends among country and drug topics to show through. NVivo was used for qualitative analysis, and to manage patterns and perform word queries for the dataset.

3.1. Data Source: Reddit

A basic search for dark-web forums revealed the Reddit forum //darknetmarkets. Although accessed through the surface web, this forum was chosen due to its high popularity in discussing dark-web topics. Data was collected from this forum before a compilation of forums on Reddit pertaining to the dark-web were banned due to site policy issues. The decision to collect most forum data from this site was based on the spread of discussions and number of comments associated with them. Postings and discussions on this forum range from product and vendor reviews, sourcing, and knowledge on trafficking drugs to activities associated with cryptocurrency and stolen credit card data. Postings categorized "Shipping & Logistics" and "Questions and Discussion" were manually picked for analysis. Data collected from each thread included: username of commenter, date posted, drug pertaining to, comment, and any notes surrounding the theme of the discussion.

3.2. Data Source: Dread

To supplement data from Reddit, comments were also chosen from Dread – an older forum that gained popularity over the past month due to users displaced by the shutdown of //darknetmarkets. As these are open forums, data collected is from buyers, vendors, and curious browsers; the dataset contains the reality and glimpse of knowledge from all perspectives.

3.3. Data source: Dream Market

Vendor profiles on Dream Market were chosen from the "drugs" front page and narrowed down based on the filters: "ships to Canada", "escrow", and "Bitcoin". The cryptomarket Dream Market was chosen due to its size and popularity [18]. On Dream Market, each vendor has their own page that gives them space to petition their product and business practices. Items on the vendor profile page include username, products, business write-up, and feedback from previous buyers. The first three pages of products were routinely checked to find vendor profiles with comments pertaining to shipping tactics. To find themes among vendors, the following data was collected from each vendor profile: vendor name, comments about shipping and stealth, product connected to the vendor, countries shipped from, key words associated with the search, and notes differentiating feedback from vendor comments. Additionally, feedback pages of vendors chosen were searched for comments on knowledge of packaging and stealth techniques.

4. Results

The sample included 71 comments and presented themes surrounding stages of a dark-web transaction: activities before, during, and after the shipment. The overall results give evidence that knowledge about trafficking drugs through the dark-web is happening. A word count was used to determine how common specific words came up in discussion. The commonality of words helped reveal the transaction stages. The words with the highest percentage of usage included: shipping, stealth, use, address, safe, and customs.

4.1. Before Shipment Activities

A transaction initiates the chain of events leading up to a delivery of dark-web drugs with vendors being the first piece in the chain. As cryptomarkets function on a platform of feedback reviews, vendors work hard to ensure themselves, their product and buyers are safe throughout the whole process. Although the comments in the forums cannot be dissociated between vendors and buyers, knowledge pertaining to the steps and details prior to shipping a parcel could be found. Users (14%) on both forums and vendor profiles emphasized details about addresses to reduce the risk of a parcel being non-deliverable, returned to sender, or lost:

> "Always use a name and address that you have used in the past and you know will get delivered. This decreases suspicion and packages that are returned as undeliverable. Returned packages are very bad as who ever receives them may turn it into LE! So please double, even triple check your address to make sure everything is correct." (Dream Market vendor profile)

As mentioned on both vendor profiles and forum pages, only the importer address needs to be legitimate and deliverable. In the sample of 71, 10 of the comments were connected to details surrounding addresses. It is up to the buyer to provide the vendor with properly formatted address information:

> "SURNAME+NAME,STREET+NUMBER, POSTALCODE+CITY, COUNTRY. Keep in mind that we copy this format directly to the label printer any wrong filled formats will make you lose your right for a refund!" (Dream Market vendor profile)

These comments detailing customs declarations technicalities are evidence that users of the dark-web understand and know the probing techniques customs and border officers utilize to "profile" parcels.

Vendors were aware that some countries hold a higher risk than others to ship drugs to. It was evident that vendors keep up with the policies and news, namely take-downs by law enforcement, to ensure they are not shipping into a hot-spot. Details regarding law enforcement actions are consistently posted on dark-web news pages including Reddit and DeepDotWeb. To ensure their business plan is clear, vendors list on their vendor profile page where they refuse to ship to and deem too risky:

> "{-----RISK COUNTRIES-----}~ NORTH & SOUTH AMERICA, Scandinavian, AUSTRALIA" (Dream Market vendor profile)

> "USA & AUSTRALIA.We do not ship to these countries."(Dream Market vendor profile)

When one Reddit user inquired about the risk of ordering to the United Kingdom [UK], the response gave a detailed outline of another user's risk scale in relation to countries:

> "NL is up near the top, USA and CAN are fairly safe but still much riskier than EU to EU. And US varies by states, shipping out of Colorado or other green states may be harder. South America, Asia and Africa are often very risky but you are probably not thinking about them anyway. For UK, domestic is obviously king, followed by safe EU countries like Spain. Then CAN, then US, then probably AUS. That doesn't mean US is a no-go, but you should be extra careful about the vendor's stealth." (Reddit forum posting)

Discussions regarding risks associated with specific countries and drugs appeared frequently throughout the data collection timeframe. Appearing irrational or paranoid, one user's theories can be turned into knowledge for another user and save them from shipping to a hot country:

> "It seems like ordering bars from Canada specifically is hotter than most Canadian transactions, just from what I've seen browsing the subs. You can thank all the fucking Canadian bulk pressers who get caught up for that" (Reddit forum posting)

Evidence of knowledge sharing on evading law enforcement was also found for the buyer role. Vendor pages give options for shipping levels associated with countries and their prices – the buyer chooses the level matching their demand for the purchase. It is evident that buyers understand the risk they are taking when purchasing the lowest level of shipping option corresponding to the shipping route of their purchase:

> "Always use domestic unless it can't be avoided. If it can't be avoided just realize you are putting an extra step between you and your package arriving undisturbed. You might be saving a few bucks but what is avoiding customs worth to you? I tend to pay a slightly higher premium just to keep the deal 100% domestic and I have no regrets about that." (Reddit forum posting)

The role of both parties and their safety appeared to be highly emphasized as an important step before shipping products. It is in the best interest of both parties to ensure they perform their role well to decrease the chances of a disrupted parcel and thus they readily share knowledge on addresses, shipping options, and risk countries.

4.2. The Waiting Game

All actions leading up to placing a shipment determine the parcel's future. Knowledge on packaging techniques to distract law enforcement from the true contents of the parcel were the most popular and emphasized topic in discussions about shipping and logistics. Although rules on cryptomarkets and forums forbid users from detailing specifics about a vendors' stealth, the topic is still a hot conversation to pick at:

> "No Stealth details. Stealth is what keeps the packages getting to you. If you describe a vendors stealth, their packages can be profiled a lot easier. Commenting on the quality of the stealth is fine, just don't get into specifics." (Reddit forum posting)

The vendors' stealth comes into play when it is inspected by customs and border officers at the importing country's mail facility. Stealth varies for each product, vendor, quantity, and destination to keep law enforcement in the dark on what parcels contain drugs:

> "The cocaine will be packed in an envelope/vacuumed and sealed with MBB.I try to ship it as rocky as possible, although small orders will most likely receive powder." (Dream Market vendor profile)"

For someone starting up a shop on a cryptomarket, research on dark-web forums would saturate their curiosity on the rules of stealth. This small sample yields evidence of buyers and vendors detailing themes and details that need to be addressed. Choosing a "fake mustache", an online personality and profile, involves research into how this lifestyle and work functions:

> "I have been a browser for about 4 months and am considering becoming a buyer from certain markets. I have been reading everthing I can find in regards to OPSEC and have tried to implement it." (Dread forum posting)

> "Nobody is going to outright say "this is how to ship some tasty illegal treats" on a public forum buddy. Best way forward is to buy some choice product (I have an excellent line in MDMA if you like that kind of thing) from a few dif vendors and if you want to go forward and sell then just choose your favorite fake mustache. Some items require specific solutions but that's about it. Dead simple." (Dread forum posting)

The use of moisture barrier bags (MBB) and alcohol dripping are two technical packaging techniques that users ensure will remove scent and trace evidence from their parcel. More specifically, 28% of the 32 vendor profile comments collected discussed the use of MBB and alcohol dripping. Most vendor profiles and feedback comments (43.8%) share with their potential buyers that they utilize stealth techniques; their ratings and feedback can attest to it. It should be noted, stealth techniques within this stage of shipping include: odor protection, MBB, alcohol dripping, and any technique to lessen the truth of the contents.

Vendors have the right to be paranoid about the future of their parcel. As the parcel travels, both parties of the transaction are at risk of law enforcement detection. As previously mentioned, if vendors are researching and implementing stealth techniques, buyers need to hold up their end of the transaction and stay discrete in their actions. A discussion curious about tracking numbers and how to check them lead one user reminding buyers:

> "17track + Tor is a safe bet I think. Only thing is it doesn't give you an Est. Delivery date like USPS.com does. But it shows movement, nonetheless.And as other have mentioned, only track it every so often, not everyday." (Dread forum posting)

The usage of Tor and tracking websites to discreetly check the status of a parcel is a key piece of knowledge that may be overlooked. With the knowledge of shipping times provided by the vendor, the status of parcel could indicate to a buyer if their parcel may have been seized, lost, or they are potentially subject to a visit from law enforcement:

> "One non-arrival could literally mean anything from a scamming vendor who never sent the order to begin with to a legitimately lost package, but two in a row is not a coincidence." (Reddit forum posting)

It could be argued that the phase where no party holds custody over the parcel is the riskiest and most important. As mentioned by one user, "Nobody is going to outright say "this is how to ship some tasty illegal treats"", but rather it is best practice if they "have been reading everything I can find in regards to OPSEC and have tried to implement it (Dread forum posting)". If customs and border officers "have data sharing between departments", dark-web users will also be working together internationally to ensure their team is a step ahead of law enforcement (Reddit forum posting).

4.3. You've Got Mail

In the best-case scenario, the parcel will arrive to the buyer and the vendor's payment will be released to them through the escrow system. In the case of law enforcement seizing a parcel, individuals can confide in their fellow dark-web users on advice how to protect themselves and their rights from law enforcement. Although a parcel's status may foreshadow a seizure, users have learned that law enforcement does not always catch everything; evidence that the knowledge of law enforcement missing things is a true reality:

> "Instead, to my surprise, the package actually arrived. But here's the weird part - it had obviously been opened and thoroughly examined. The vendor has used four layers of stealth. Every layer had been carefully slit open with an obviously very sharp knife, and then just as carefully taped back up and then sent on its way." (Forum posting)

In the scenario of a seized parcel, "They buyer is the one that needs to be concerned. Drugs floating around with their name on it (Forum posting)." Knowledge about interacting with law enforcement and actions to take concerning a seized parcel were found in 17.9% of forum postings collected. The terminology "love letter" was found used by multiple users to describe a letter from customs and border patrol acknowledging that the individual's parcel had been seized because of drugs

within the parcel. In addition, it was learned through a thread that a "burned address" refers to an address that no longer can be used due to law enforcement having knowledge it may have drugs being shipped to it:

> "CD or LL. Only other reason to not receive either of those is they're watching you, which is why you don't flood your drop and you switch your drops up. I probably have a lot of drops I consider burnt that realistically aren't but at the end of the day that's up to you to rather be safe than sorry." (Reddit forum posting)

This user describes the use of a "drop" and contemplates whether their drop is still reliable. A "drop shipment" is the usage of a third party for shipment while the vendor never has contact with the goods. Knowledge pertaining to drop shipment allows vendors to read risk levels more efficiently. Alternatively, tips are provided for controlled deliveries; the delivery of a seized parcel by an undercover officer to catch the importer. Comments suggest the individual deny the parcel and not acknowledge knowing the contents:

> "yeah it's probably seized but you actually unfucked yourself by not signing for it lol. They couldn't pop you for it. Denie everything and clean house. You know nothing about this package and weren't expecting it." (Reddit forum posting)

> "Ive had police come to my door. I never received a notice at all. They left a buisness card and on the back it said "We have a problem" I never responded as I dont have problems. This is in the US" (Reddit forum posting)

As paranoia sets in, it is discussed that a buyer must remember their actions and behaviour may be under surveillance. As one would assume, the more illicit and larger quantity shipments hold higher stakes. At this point, it is up to the buyer to research and understand the difference between normal and suspicious behaviour. It has been suggested individuals:

> "Don't be waiting at your mailbox everyday go and get the mail later on. Don't do anything suspicious that'll make your mail deliver raise a red flag. All it takes is for them to report to their supervisor that a specific address has been receiving many packages mailed from strange places." (Forum posting)

5. Discussion and Implications

5.1. Shared Goal

Vendors and buyers do not have the obligation to warn each other about risks associated with drug trafficking on the dark-web, however the above evidence shows that for a community to function everyone must help their neighbor. In the sample of 71, among others, a key theme was a shared goal:

> "You really should post who the vendor was to help others avoid ordering from them and getting packs seized. That's the point of these forums, coming together as a community to inform and help the other members." (Forum posting)

Sharing knowledge on their experience on the dark-web is how their shared goal comes to life - profiting, getting their product, and all parties remaining safe. To understand why cryptomarkets consistently regrow after law enforcement infiltration is to understand that drug dealers and buyers are the main source of dark-web knowledge.

It has been suggested that law enforcement and the government invest in specialized units and software that focus on analyzing the knowledge within conversations regarding trafficking of drugs on the dark-web [24][14]. Are jurisdictions, nationally and internationally, working together with a shared goal and agenda? Is a general blanket answer being applied to all jurisdictions or should an overseeing group designate a shared goal to different regions and jurisdictions? In a sample of 32 vendor profiles, 10 specific countries were listed as exporting countries of drugs. This is evidence that the activities occurring on DNM is a global issue needing global cooperation. A unified goal and communication among international agencies is to collectively have an impact against a more unified global network. Without a transparent agenda, law enforcement and the government will fall farther behind the users of the dark-web.

As previously mentioned, the pilot project carried out by CBP and USPS concerning the exploitation of the US postal system presented a lack of transparency between agency goals [19]. It's suggested that the first step on unifying a goal is to have multiple agencies on board together [19]. Secondly, all agencies involved need to establish and cooperate on a goal. A means of measurement for success of the goal should be established and agreed upon by all parties involved [19]. Monitoring the dark-web is a large field of research that cannot be taken on by a single party. The establishment of transparent and unified goals among agencies will allow agencies to, at minimum, garner the same shared knowledge base as vendors and buyers.

5.2. Knowledge is Power

It is common knowledge that those with relevant knowledge tend to hold power over those without.

Keeping knowledge out of the hands of the opposing party allows you to have the ability to hold them where you want them. In the case of this research, users of the dark-web are keeping law enforcement behind them in terms of knowledge on drug trafficking. However, it may be argued that law enforcement is assisting dark-web users' strategy by not investing the proper tools, resources, and time into themselves to jump ahead in this "knowledge race".

Although this research only covers a small portion of comments, feedback, and vendor profiles found on the dark-web, the data collected is a snapshot of the extent of knowledge being shared. The data shows no boundaries for knowledge, with some users even commenting their own journey to becoming a vendor through learned dark-web knowledge. The communities online "enable information sharing for reducing the risks posed by law enforcement to illegal drug trading" and in turn foster more successful vendors and buyers [1]. With 25.5% of 5,565 American participants and 7.1% of 3,155 Canadian participants on the 2017 Global Drug Survey reporting having done drugs from the dark-web, it is clear that laymen can access the dark-web and learn from it.

5.3. Forgotten pieces

The physical side is the most vulnerable phase of the transaction and the emphasis placed on stealth packaging techniques shows acknowledgment of the risks associated with the transactions. Comments detailing risk countries, risky behaviour, and computer security measures are important, however the physical side of drug trafficking through the postal system is where seizures are more likely to happen. Data collected in this research on packaging and stealth techniques is consistent with previous studies examining general dark-web trafficking and studies characterizing purchases from selected countries [21][1][4][6]. Techniques mentioned in comments included: MBB, alcohol dripping, latex gloves, printed labels, decoys, and generic letter mail. The physical parcel is the most vulnerable piece of the process because unknown characters come into play and handle the parcel.

The stealth level of packaging techniques is vital to become a successful vendor; vendor reputation is built upon completed transactions [9]. Commonly on vendor profiles, vendors would assure buyers of their confidence in the stealth techniques they utilize. Not only is this an attempt to assure buyers of their professionalism and business quality, it is also a message that they have more than adequate skillful knowledge on the business they transact in. One could theorize that ordering from a vendor would provide the buyer with knowledge on the vendors' stealth techniques and shipping tactics. Although ethical dilemmas may ensue, packaging could be used as "evidence to better understand sellers 'practices' [21]." The parcel can connect packaging techniques with geographic profiles, importers and exporters, and drugs. Results from this research shows vendors take extensive steps to lessen the chances of law enforcement actions. Collecting knowledge specifically from vendor profiles and forums would give law enforcement intelligence to assist in parcel targeting.

5.4. Going Postal

These findings supplement the theory that the postal system is a piece of government infrastructure being exploited. No longer is trafficking drugs through the mail a theory, but reality. A key reason behind the postal system's success in drug trafficking is the international connection it holds. Anonymously and seemingly undetectable, vendors and buyers can carry out their habits and business ventures on a global level; a global business educated by a global platform, the dark-web [14].

The recent report by the Committee on Homeland Security and Governmental Affairs on the exploitation of the American postal system backs up the evidence found in this research [19]. The report reiterates the need for a new course of action to dismantle drug trafficking through the postal system. Others recommend attacking the mode of delivery for drugs [8]. As previously mentioned, 10 countries were mentioned as exporters of drugs within our sample of 32 vendor profiles. This is evidence that vendors are not worried about seizures while using the postal system for international shipments. It is theorized that reinforcing the postal system and customs and border patrol would decrease the number of international shipments being made.

6. Conclusions

Knowledge of drug trafficking through the dark-web has been well researched and documented, however the area of knowledge-sharing on drug trafficking has minimal to near no research. Aldridge and Askew's (2017) article on risk reduction and delivery dilemmas is the most recent and relevant research relevant to the study of the knowledge-sharing network on the dark-web [1]. The research outlined in this paper attempts to highlight a topic that some may feel law enforcement is neglecting: dark-web knowledge sharing.

The level of research law enforcement and the government have conducted on the dark-web is unknown, but the current available research does not put forth evidential support in the same field as this paper does. The first course of action recommended to law

enforcement and governments is to collectively agree on a goal and transparent plan for the issue. As previously mentioned, dark-web users are working together as a collective group to defy law enforcement. Sharing knowledge between international nation-states is a necessity to beat cryptomarket users. Both the importer and exporter countries need to collaborate on legislation and strategies as the dark-web is too vast for a single entity to investigate alone.

Secondly, governments should invest in big data technology. Crawling software would allow researchers to pick out key language on the dark-web associated with knowledge on shipping drugs internationally to build an up-to-date library of trends and knowledge [14][24]. The intelligence generated from this technology would assist customs in targeting parcels with suspected drugs. Data presented in this paper gives evidence that knowledge is being shared. It is unknown if the knowledge shared on the dark-web is legitimate and useful, however it is best to collect all knowledge relevant to the topic.

Thirdly, attacking the services directly has proven useful (eg. AlphaBay, Hansa, Silk Road), however this action displaces vendors and buyers to a new market and does not fix the problem. As cryptomarkets are built on a foundation of trust, it is theorized that destruction of the feedback system could potentially jeopardize multiple vendors' businesses. It is unknown how feasible flooding vendor profiles with negative feedback is, therefore this recommendation would need to be paired with more research.

Overall, the interpretation of the data collected is that the criminals are winning. Although the online drug trade only accounts for a small percentage of the global drug trade, the popularity of cryptomarkets is increasing steadily [5]. As drug trafficking moves online, law enforcement needs to also take the step to move online. The implementation of policy is recommended because of the impact it can have as a "scare tactic". However, it should be cautioned that policies may not help better understand the system of international drug trafficking through the dark-web.

The final recommendation is for law enforcement to understand their strengths. Vendors and buyers online understand that the physical side of drug transactions is the most vulnerable stage. Law enforcement needs to capitalize on this strength because "information online has significant implications for the effectiveness of postal interdiction regimes [15]" The techniques currently in place to detect and inspect parcels should be supplemented with intelligence gathered from knowledge shared online. As criminals have learned and adjusted their practices around law enforcement, it is recommended law enforcement does the same. The knowledge gap between the two parties could be lessened with more resources and research on knowledge from the dark-web.

As activity on the dark-web increases, law enforcement has two courses of action to take: continue to shut down and displace cryptomarkets or invest in research to understand the knowledge being shared online and implement it into the postal system. This research gives evidence that there is an international knowledge sharing network on the dark-web law enforcement should be analyzing. Comments range from techniques on packaging and address formats to how to ship specific drugs and risks associated with countries. Attacking dark-web services provides a short-term impact, however it does not advance law enforcements intelligence on how international drug transactions are carried out. Focus should be placed on the physical aspect of drug trafficking – the postal system. Paired with intelligence from analysis of online knowledge, parcel targeting will allow law enforcement to increase seizures and build their own knowledge network; a network connecting vendors, buyers, drugs, and countries to packaging techniques.

7. References

[1] Aldridge, J., & Askew, R. (2017). Delivery dilemmas: How drug cryptomarkets users identify and seek to reduce their risk of detection by law enforcement. *International Journal of Drug Policy, 41*, 101-109. Doi: https://doi.org/10.1016/j.drugpo.2016.10.010

[2] Aldridge & Décary-Hétu (2016). Hidden wholesale: The drug diffusing capacity of online drug cryptomarkets. *International Journal of Drug Policy, 35*, 7-15. Doi: https://doi.org/10.1016/j.drugpo.2016.04.020

[3] Aliens, C. (2018). Reddit just banned /r/darknetmarkets – biggest darknet subreddit. Retrieved from https://www.deepdotweb.com

[4] Bancroft A., & Reid, P. S. (2016). Concepts of illicit drug quality among darknet market users: Purity, emobodied experience, craft and chemical knowledge. *International Journal of Drug Policy, 35*, 42-49. Doi: https://doi.org/10.1016/j.drugpo.2015.11.008

[5] Barratt, M., Ferris, J. A., & Winstock, A. R. (2016). Safer scoring? Cryptomarkets, social supply and drug market violence. *International Journal of Drug Policy, 35*, 24-31. Doi: https://doi.org/10.1016/j.drugpo.2016.04.019

[6] Broséus, J., Rhumorbarbe, D., Mireault, C., Oullette, V., Crispino, F., & Décary-Hétu, D. (2016). Studying illicit drug trafficking on Darknet markets: Structure and organization from a Canadian perspective. *Forensic Science International, 264*, 7-14. Doi: https://doi.org/10.1016/j.forsciint.2016.02.045

[7] Camille, B. (2017, September 18). RCMP says charges to be laid in Canada involving fentanyl shipments from China. *The Canada Press*. Retrieved from https://search-proquest-com.proxy.lib.sfu.ca/docview/1940479252?rfr_id=info%3Axri%2Fsid%3Aprimo

[8] Christin, N. (2013) Traveling the Silk Road: a measurement analysis of a large anonymous online marketplace. In the 2013 Proceedings of the 22nd international conference on World Wide Web. Pages 213-224. Switzerland

[9] Cox, J. (2016). Reputation is everything: The role of ratings, feedback and reviews in cryptomarkets.In EMCDDA, *The Internet and drug markets* (Ch.5). Retrieved from http://www.emcdda.europa.eu/system/files/publications/2155/TDXD16001ENN_FINAL.pdf_en

[10] Deepdotweb (2013, Novemeber 26). Point for safe shipping. Retrieved from https://www.deepdotweb.com

[11] Deepdotweb (2015, March 18). Evolution marketplace exit scam: Biggest exit scam ever?. Retrieved from https://www.deepdotweb.com

[12] Gilbert, M., & Dasgupta, N. (2017). Silicon to syringe: Cryptomarkets and disruptive innovation in opioid supply chains. *International Journal of Drug Policy, 46*, 160-167. Doi: https://doi.org/10.1016/j.drugpo.2017.05.052

[13] Heintz, L. (2012), 'Here's the indictment that blew the lid on the eBay of drug trafficking this week', Motherboard 20/4/2012. Available at: http://motherboard.vice.com/blog/here-s-the-indictment-that-blew-the-lid-on-the-amazon-ofdrug-trafficking-this-week

[14] Kruithof, K., Aldridge, J., Décary Hétu, D., Sim, M., Dujso, E., & Hoorens, S. (2016). *Internet-facilitated drugs trade: An analysis of the size, scope and the role of the Netherlands.* Santa Monica, CA: RAND Corporation.

[15] Martin, J. (2014). *Drugs on the Dark Net: How cryptomarkets are transforming the global trade in illicit drugs.* London: Palgrav Pivot. Retrieved from https://link-springer-com.proxy.lib.sfu.ca/content/pdf/10.1057%2F9781137399052.pdf

[16] Mounteney, J., Oteo, A., & Griffiths, P. (2016) The Internet and drug markets:shining a light on these complex and dynamic systems. In EMCDDA, *The Internet and drug markets* (Ch.1). Retrieved from http://www.emcdda.europa.eu/system/files/publications/2155/TDXD16001ENN_FINAL.pdf_en

[17] Popper, N. (2017, July 18). Hansa market, a dark-web marketplace, bans the sale of fentanyl. *The New York Times.* Retrieved from https://www.nytimes.com

[18] Popper, N., & Ruiz, R. (2017, July 20). 2 leading online black markets are shut down by authorities. *The New York Times.* Retrieved from https://www.nytimes.com

[19] Portman R., & Carper, T. (2018). *Combatting the opioid crisis: Exploiting vulnerabilities in the international mail.* Retrieved from the Committee on Homeland Security and Governmental Affairs Senate website: https://www.hsgac.senate.gov/imo/media/doc/Combatting%20the%20Opioid%20Crisis%20-%20Exploiting%20Vulnerabilities%20in%20International%20Mail1.pdf

[20] Public Works and Government Services Canada (2017). Canada's postal service: A historical overview. *Government of Canada.* Retrieved from https://www.tpsgc-pwgsc.gc.ca

[21] Rhumorbarbe, D., Staehil, L., Broséus, J., Rossy, Q., & Esseiva, P. (2016). Buying drugs on a Darknet market: A better deal? Studying the online illicit drug market through the analysis of digital, physical, and chemical data. *Forensic Science International, 267*, 173-182. Doi: https://doi.org/10.1016/j.forsciint.2016.08.032

[22] Shedding light on the dark-web. (2016, July 16). *The Economist*. Retrieved from https://www.economist.com/news/international/21702176-drug-trade-moving-street-online-cryptomarkets-forced-compete

[23] Southwick, R. (n.d.). Inside the dark-web drug trade. *CBC News*. Retrieved from https://newsinteractives.cbc.ca

[24] Steffen, G. S., & Candelaria, S. M. (2010). Drug parcel systems. *Drug Interdiction* (2nd Ed.). Retrieved from https://doi-org.proxy.lib.sfu.ca/10.1201/b13778-11

[25] Vajgert, G. (1996). Profiling postal packages. *The Free Library*. Retrieved from https://www.thefreelibrary.com/Profiling postal packages.-a018447923

[26] Vinton, K. (2014, November 7). So far feds have only confiremd siezing 27 "dark market" sites in operation onymous. *Forbes*. Retrieved from https://www.forbes.com

[27] van Hout, M. C., & Bingham, T. (2014). Responsible vendors, intelligent consumers: Silk road, the online revolution in drug trading. *International Journal of Drug Policy, 25*(2), 183-189. Doi: https://doi.org/10.1016/j.drugpo.2013.10.009

[28] von Slobbe, J. (2016). The drug trade on the deep web: a law enforcement perspective. In EMCDDA, *The Internet and drug markets* (Ch.8). Retrieved from http://www.emcdda.europa.eu/system/files/publications/2155/TDXD16001ENN_FINAL.pdf_en

[29] Winstock, A., Barratt, M., Ferris, J., & Maier, L. (2017). *Global Drug Survey 2017*. Retrieved from https://www.globaldrugsurvey.com/wp-content/themes/globaldrugsurvey/results/GDS2017_key-findings-report_final.pdf