

Dark Web Markets: What can they teach us?

Stijn Nijhuis
University of Twente
P.O. Box 217, 7500AE Enschede
The Netherlands
s.p.g.nijhuis@student.utwente.nl

ABSTRACT

A business that strictly uses the dark web as its sales medium, such as an illegal drugs web store, faces different challenges than a legitimate business that must meet applicable legal requirements. These Dark Web Markets (DWMs) have to take extra precautions to prevent their online stores from being shut down. Complete anonymity and privacy are necessary to complete a transaction, as every step of the supply chain needs to stay hidden from the public. The data also has to be handled with extreme care; data leaks can lead to serious consequences for anyone involved. The practices necessary to safeguard this data can be of value for legitimate businesses. Hence, the goal of this research is to analyse the supply chain and data management practices of DWMs and examine what can be applied to legitimate businesses. The contributions of this paper lie in the practices or processes found that can be used to improve legitimate businesses, as well as provide a foundation for further research into the matter.

Keywords

Dark web, Dark Web Market, drug vendors, supply chain, business process

1. INTRODUCTION

Almost two decades ago, the three Americans Roger Dingledine, Paul Syverson, Nick Mathewson started working on a project named The Onion Routing (TOR) [1]. Paul Syverson worked at the U.S. Naval Research Lab on what now could be called the foundation of TOR, namely Onion routing [2]. The goal of the TOR project was to maximize privacy on the internet. Dingledine, Syverson and Mathewson achieved this by creating a network of relays. A standard connection to the TOR network consists of a virtual circuit with three randomly selected relays [3]. Every step in this circuit is encrypted, making it nearly impossible to identify the source of the data package or the one who tries to access the data package.

In 2002, when the initial version of the TOR browser deployed, anonymous browsing got more accessible to the public. This software has always had the intention of facilitating safer online communication. The usage of TOR

for illegal purposes is simply an unfortunate side effect that was bound to happen. The first online drug store on the dark web opened in February 2011 under the name Silk Road. "A place where you can log in and order marijuana to LSD, which will be delivered on your doorstep by the US Postal department, obviously clueless after you pay for the drug through bitcoin" [4]. Silk Road showcased the potential a business on the dark web has before the FBI was able to build a case in 2013 [5]. The case also revealed the before unknown power of the TOR network as even the arrest was caused by human errors and not a flaw within the system.

Silk Road is seen by many as the pioneer of DWMs. After Silk Road got taken offline in 2013, more marketplaces opened up, from other drug stores like Agora and Utopia to arms dealers and software exploit sellers. One flaw that Silk Road revealed, however, is that the protection TOR offered online is not enough. For a DWM to flourish, every aspect of the business must be managed and secured.

This research intends to uncover the processes and practices that these businesses use. The data handling and supply chain have to be first-class, as the margin of error for these businesses is extremely slim. A simple mistake can have serious consequences. The increased magnitude of said consequences forces a DWM to improve its methodology. Therefore, there might be practices or processes that can be used to improve legitimate businesses.

2. PROBLEM STATEMENT

Preventing data leaks, improving customer service, maintaining the reputation and integrating new technologies are challenges that businesses face today. Even the largest companies struggle with these challenges from time to time. Some well-known examples are Facebook's data leak in 2019, LinkedIn's inadequate customer service [6] or Ford's failed digital transformation[7].

However, these companies remain some of the world's largest companies even after the mistakes they have made. In comparison, the seizure of DarkMarket after a server hack [8] caused the business to be completely shut down. This showcases that the corporations do not have the same urgency to prevent these issues from happening, as the consequences differ.

2.1 Research Questions

The problem statement will guide us towards the following research question:

What can legitimate businesses learn from DWM practices or processes?

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

36th Twente Student Conference on IT Febr. 4th, 2022, Enschede, The Netherlands.

Copyright 2022, University of Twente, Faculty of Electrical Engineering, Mathematics and Computer Science.

To answer the main research question, the following sub-questions will be of help:

1. How does one define a legitimate business?
2. What are the added challenges a DWM has to face in comparison to a legitimate business?
3. How does a DWM facilitate an illegal drugs supply chain?
4. What (data) practises are conventional for DWMs?

3. METHODOLOGY

The first sub-question can be answered by looking at the core functionalities of Silk Road and Hydra. These functionalities can be used to make a connection to a comparable legitimate business. The data archive by Gwern et al. [9] includes the listings of Silk Road, while Hydra is still online on the TOR Network. A study by Ilpoekr [10] also gives more insight into Hydra. After this analysis, a comparison between DWMs and comparable legitimate businesses can be made to clarify the definition of a legitimate business.

To answer the sub-questions about the added challenges and the supply chain of a DWM, secondary data analysis is required. As the point of a DWM is to stay hidden from the public, information is scarce. In addition, the TOR browser deprecated V2 Onion links in July 2021 and moved on to the longer, more secure V3 Onion links. The websites that have not yet converted to V3 are unavailable, limiting the available sources on the dark web even more.

Due to the scarcity of information, grey literature has to be analysed. The definition of grey literature according to the National Research Council [11] is "literature that is not 'white' (available and cataloged), and that is not 'black' (not available, unknown, or not obtainable)". For example, a popular distribution channel for hackers that can also be a source of grey literature is Pastebin. Pastebin is used by hackers as it is a platform where they can share source code, data leaks, and dark web links anonymously. These Pastebin links are then shared through forums.

In addition to the grey literature that can be found via forums, Google, and the dark web search engine Haystak, previous research on the dark web can also be analysed. These papers are found using Google Scholar. To select these papers, the following exclusion criteria has been defined. Research before 2011 is excluded, as Silk Road was founded in 2011; the standards of the DWMs today are set by Silk Road, making the DWMs prior to Silk Road otiose. Research papers that are not accessible are also excluded. After the exclusion criteria is defined in Google Scholar, the search queries were entered. For more information on the tor browser, the query "tor browser analysis OR research" was used. To gather more information on the DWMs, the search query "drug market drugs OR illicit OR anonymous". Then, to select the relevant papers for this research the title, abstract and conclusion were read.

In addition to the data archive by Gwern [9], the grey literature or articles and, the literature found in Google Scholar, relevant research cited in previous found literature was added. These sources were analysed to use Porter's value chain analysis tool to obtain a better understanding of one of the largest DWMs on the market. Getting a better understanding of DWMs is necessary to see the differences between a DWM and a legitimate business.

After the general workings of a DWM are studied, it might be feasible to determine how one separates itself from the competition. The online drug stores predominantly sell the same products to the same markets. Therefore, a difference in customer support, pricing or availability of the product will be present. A lot of the major DWMs can be analysed to view the features they offer. Afterwards, a comparison can be made to determine if the price difference is substantial enough to make a difference, or that the additional features on the store are the reason a DWM is more attractive to customers. This will make it possible to filter out the stores that outperform the competition in terms of features, which are the stores that are worth researching to find better practices.

To answer the final sub-question, it is worth looking at how dark web stores are created in the first place. Are there store builders available? Is it better to code the store from the ground up? Regarding the second option, how do you handle the data on the dark web? To find the answers to these questions data analysis or prototyping is needed. Data analysis can be done in the form of studying cases of seized stores such as Silk Road and DarkMarket. In addition, a mock store can be built using a store builder, if available, to test the back-end functionalities first-hand.

Finally, to answer the main research question, the data gathered from the sub-questions can be analysed to form an overview of the best practices in DWMs. The practises can then be examined to see if they are feasible to implement in legitimate businesses.

4. RELATED WORK

There have been several considerable contributions to the research of DWMs. These contributions include, for example, massive datasets containing over 80 complete DWMs, which was made by Gwern et al. [9]. In addition, papers were written about the relation between the exchange rate of Bitcoin and drug prices by Zaunseder and Bancroft [12]. However, no previous research regarding the business processes of a DWM has been published yet. The papers that follow are, to a certain extent, all related. They do not directly relate to the business processes of a DWM, but they do give more insight into the workings of DWMs.

Gwern et al. [9] have created the largest available collection of DWMs. It contains over 80 DWMs, more than 37 related forums and has a total size of about 1.6TB uncompressed. This dataset has been used in a wide range of research papers. Some of these papers used this dataset to get a better understanding of the working of a DWM.

Zaunseder and Bancroft [12] have researched the relationship between the prices of drugs and the exchange rate of Bitcoin. This helps to understand how the prices on the markets are formed by evaluating the influence of an external factor such as the price of a cryptocurrency.

Christin [13] researched Silk Road. The products sold and revenues made by sellers and Silk Road operators are both parts of the analysis. This paper could help examine how a DWM was able to steadily grow during the time it was online.

Rhumorbarbe et al. [14] analyse the Evolution market as well as the packaging and purity of their products. Their analysis greatly aids the understanding of the practices at the end of the supply chain. In addition, their comparison between the information online and the received products showed that the digital information seemed, at least to the extent of their research, accurate.

Kilmer and Hoorens [15] analysed the indicators for improving the understanding of DWMs. To recommend indicators, one first has to understand the market itself. Therefore, the research conducted on the market by Kilmer, Hoorens and RAND can be of added value to this research.

Li et al. [16] researched the supply chain of opioids on DWMs. This has been done to get a better understanding of anonymous markets. Public health officials and other stakeholders can use the information on the DWMs to figure out methods to counter the current worldwide opioid crisis. However, the research focused on the supply chain of the supplier is of great value to this research; it aids to create an overview of the entire supply chain.

5. RESULTS

The results of the research can be split up into three sections regarding the sub-questions. The sub-questions are answered according to the determined methodology. However, due to the availability of information regarding the dark web, slight deviations from the methodology were necessary.

5.1 Legitimate Businesses

First, a baseline has to be established before we can compare legitimate businesses to DWMs. The legal definition of a legitimate business: "a lawful business enterprise operating in compliance with federal, state and local law". However, this is too broad for this research as it includes almost every corporation. To narrow it down, the core functionalities of a DWM can be used to find comparable legitimate businesses. As the DWMs only sell their products online, the relevant legitimate businesses are assumed to be e-commerce stores. In essence, large DWMs such as Silk Road and Hydra are marketplaces for vendors to sell their goods. The DWM offers support and manages the transactions between the vendor and the customer. Thus, two close comparable legitimate businesses that are similar in structure to Silk Road are eBay and Amazon [17].

If we take a look at the functionalities of both Silk Road and Amazon, the resemblance is striking: Both are websites where you can order goods sold by vendors, with the guarantee and support of the overarching marketplace. After the order has been placed and is paid for, the goods are shipped to the customer. If there are any problems, the marketplace can be contacted who will, in turn, solve them with the vendor. A review can be placed by the customer after the goods are received to boost or lower the reputation of the vendor based on its performance. The main difference seems to be the type of products that are sold on both stores and the consequences that comes with the type of products.

An important difference that has to be mentioned, is the difference between a comparable legitimate business and a legitimate business that can benefit from the outcome of this research. A comparable legitimate business is used to provide a baseline for the practices or processes that are used by DWMs, as the process of a transaction at Silk Road is similar to a transaction on Amazon. However, if a DWM uses a method or process that is not limited to these type of e-commerce stores, such as good data practice, it can be beneficial for regular e-commerce stores as well. Thus, the comparison between DWMs and comparable legitimate businesses is only necessary to identify the differences and does not limit the applicability of the potential improvements this research showcases to those businesses.

5.2 The added challenges of a DWM

To answer the first sub-question "What are the added challenges a DWM has to face?", a literature review was the selected approach. To start, there are a few obvious challenges that do not apply to legitimate businesses. As it is regarding illegal drug stores, a DWM has to prevent law enforcement from seizing its webshop. Thus, the data of its employees, as well as the data from its customers, need to be stored properly; any data leak or hack leads to severe criminal charges.

Nachash, the former owner of a large document sharing and publishing dark website Doxbin [18], shows insight into the configuration of a DWM via Pastebin [19].

Nachash explains the start-up process of a DWM, for both the legal and technical aspects. The legal part of Nachash's article is not relevant, as the goal is to find applications for legitimate businesses; illegal methods to hide from law enforcement are not applicable. Therefore, the analysis will be done on the technical part of the article.

Encryption is the main point, as any information regarding a DWM has to be secured properly to prevent the website from being seized. But even though legitimate companies also want to safeguard their information, they do not tend to match the encryption levels of a DWM. One example is email usage. Most legitimate companies rely on Gmail or Hotmail as the standard communication tool. Both services are expected to be safe, as the emails get encrypted by default via the HTTPS protocol. However, Microsoft and Google both have access to the content of the mail sent via their respective services. In addition, research by Babrahem et al. [20] provides evidence that these services are also not secure enough from external attacks. Thus, for optimal safety, another layer of encryption has to be added. The most accessible option is to encrypt the content of an email via end-to-end encryption. Reuter et al. [21] mentioned and user-tested three different major end-to-end encryption technologies, namely PGP, S/MIME, and pEp. The test included installing and configuring the encryption tool and sending a secure email. The result of the test was that while PGP and S/MIME are impractical to use due to the management of the encryption keys and the difficult configuration, pEp showed potential for daily use. This showcases that while encryption tools are available, and applicable, for everyday use in legitimate businesses, it does not seem to be the standard whereas it is essential for DWMs.

Apart from the technical and legal aspects, another issue the dark web presents is trust. As the entire idea of the dark web is to stay anonymous, proving that a DWM is trustworthy is quite difficult. To build up this trust, a lot of DWMs start by price-matching already established sellers, or by selling at a loss in the beginning. Some even go as far as adding free samples as proven in the research of Ladegaard [22]. The two extra pills in the third order of Rhumorbarbe et al.'s research [14] also showed that the sellers add free samples to already buying customers. These free samples are used to build up or increase customer loyalty. Once the initial trust has been established, ratings and overall service become key.

A study by Christian [13] showed that on Silk Road during the time it was online, a 5/5 star rating was given after 96,5% of the reviewed transactions. Although Christian cautioned to not interpret that result too quickly as there are also "out of escrow" transactions that do not get a rating, there is a valid reason why this rating is very high. Research conducted by Tzanetakis et al. [23] shows

that reputation is key, as DWMs with a great reputation attract more buyers. To achieve this, trust is proactively promoted by the administrators via support and market structure, and by the vendors via "good conduct".

5.3 Hydra's value chain

For the second sub-question "How does a DWM facilitate an illegal drugs supply chain?", Porter's value chain analysis has been done on Hydra. As a lot of different DWMs sell the same products, the reason why Hydra is one of the largest DWMs in the world might be more complex than solely a lower price. Porter's value chain analysis focuses on the primary and support activities with the customer as the main principle. Thus, this analysis tries to unearth how Hydra achieved to become Russia's largest DWM by taking a closer look at its supply chain.

Porter's value chain analysis consists of two components which in turn are divided into sub-components. The primary activities include operations, inbound and outbound logistics, marketing and sales, and service. The support activities include firm infrastructure, technology development, human resource management and procurement. To research these aspects of Hydra, the Onion website of Hydra was analysed. For additional information, a research about Hydra's drug sales in Russia by Ппоект (Project) [10] was consulted.

Hydra's Primary Activities: The primary activities represent all the activities that contribute to Hydra's services directly. These do not include indirect activities. There are five primary activities in Hydra's value chain analysis model namely inbound logistics, operations, outbound logistics, marketing and sales, and services.

Operations: Hydra's operations consist of two components to create the finished service/products. The first includes the technology to facilitate the buyers and sellers of all the products. This marketplace is the primary source of operations for Hydra. The second component involves the same marketplace, but with Hydra as the direct seller. The difference here is that Hydra needs to handle the products too, instead of solely being the middleman. The margins are greater when they sell products themselves in comparison to the commission from the other sales. Thus, even though this is not the primary source, it is the more profitable source.

As the store is available only on the Dark Web, there is a protocol for buying as well as selling on Hydra's marketplace. A complete transaction process including the creation of a store is as follows:

1. Seller buys and creates a store on Hydra
2. Seller adds products to said store
3. Buyer tops up their Hydra bitcoin balance
4. Buyer buys or pre-orders the product using their bitcoin balance (pre-order: the product will be manufactured after the order is placed)
5. The balance is instantly withdrawn from the Buyer's balance
6. Seller gets notified of the order
7. Seller sends the location of the product to the buyer
8. Buyer picks up the product from location
9. *If there are issues with the product, the Seller can be contacted for clarification or a replacement product.*

10. Seller receives the payment from Hydra

Inbound logistics: The inbound logistics for Hydra are a bit unconventional in the sense that they do not store the products they sell themselves. However, it does include the hosting of the online platform. To do so, Hydra needs servers and a wide range of other hardware products. Even though the webshop is running on the TOR network, the operational requirements are similar to a regular webshop.

In addition to the technical aspects of the webshop, Hydra also hires growers and chemists for their own stores. This allows them to generate a regular stream of products which in turn allows for better availability of products, leading to a competitive advantage. As the warehousing needs to stay hidden from the public, not much information can be found on this. However, given the amount of readily available products, this seems to be better organized than most competitors.

Outbound Logistics: The outbound logistics for Hydra are unique in comparison to their competitors in the sense that they do not ship their products. Shipping illegal goods can lead to the products being intercepted by law enforcement. To prevent this from happening Hydra found a solution that gets the product from the seller to the buyer without using a delivery service. This is done by creating so-called "treasures". Treasures are products that are hidden/buried somewhere in the neighbourhood of the buyer. The buyer then gets the location of said treasure after the payment has been made. By using this method Hydra gained an edge over the competition as they have significantly fewer products that are intercepted. This led to an increase in customer satisfaction as more customers got their products.

Marketing and Sales: Hydra's "marketing" goes further than just CRM and advertising. To clarify, Hydra spent a fair amount of time and resources to take down the competition, which in this case was RAMP (The Russian Anonymous Marketplace). After becoming a monopolist in the Russian market, Hydra still spends almost 1 billion rubles (11,7 million euros) a year on marketing according to Lenta. Not only on the darknet but also in the form of advertisements, infographics and videos on YouTube and Telegram. An example of such an advertisement can be found on YouTube titled Реклама hydra 2019.

Service: Hydra stands out in the service department. They have created a forum to answer questions from both customers and sellers, as well as dedicated tickets in case a transaction goes wrong. Hydra is also involved in the selection of sellers; not everyone is allowed to sell on Hydra. In addition, the cost to create and manage a store on Hydra is around 1200 euros a year. This steep buy-in helps to prevent scams. Hydra also offers a "middleman" option, where the money goes through Hydra and only reached the seller when the buyer confirms reception of the product.

What could also be considered a service, is an integrated bitcoin exchange. The simplification of the buying process of Hydra in addition to the extended service they provide is a key factor as to why Hydra outperforms their competition.

Hydra's support activities: Support activities are in place to support the primary activities and do not directly relate to a company's products or services. The support activities can be divided into four categories: firm infrastructure, technology development, human resources, and procurement.

Firm Infrastructure: The infrastructure of Hydra is hidden to safeguard the identity of the owners and employees. Therefore, only estimations and assumptions are possible in this regard. However, as the marketing, service and sales are all top-notch, there is no doubt that Hydra has a solid firm infrastructure regarding their store.

Technology Development: Hydra keeps improving their webshop by adding new functionalities, as well as modernizing the existing features. An example of this is the integration of their Bitcoin exchange. This integration is a novelty among the DWMs. Hydra also managed to create a stable and secure environment that has yet to be cracked, which can be seen as another major advantage as other large DWMs have suffered from DDoS attacks or even full website seizures.

Another major advantage is that Hydra managed to create a stable and secure environment that has yet to be cracked, while a lot of other large DWMs have suffered from DDoS attacks or even full website seizures.

The technology development of Hydra has proven to be one of the key factors next to the service they provide to their customers and sellers. It has given Hydra the ability to keep improving their store whilst also keeping the current business at a high level.

Human Resources: The owners and managers of Hydra are all hiding their identities, so not much can be said about them. However, Hydra is actively looking to expand its business. To do so, Hydra has its own “academy” to train its employees. There are vacancies specified on the website with the positions that are currently open. This includes, for example, a position at its cybersecurity team or customer support. Unfortunately, any information about the working conditions is also hidden and the employees have not come forward with that information to the public yet.

Procurement: Procurement is only a small part of Hydra’s business model, as most of the income is through the commission and rent of the stores on its webshop. Therefore, it is not necessary to buy the products themselves, which means that the procurement department of Hydra is not where a competitive advantage can be found.

Conclusion: Currently, Hydra is (one of) the largest DWMs in the world. Even though this is an illegal online drug store, the methodology it uses to outperform the competition as a business can be very valuable to legitimate businesses. A few key components that lead to this superiority are excellent management, quality service to both customers and sellers and innovative implementations of new technologies. Hydra managed to monitor and control every aspect of its business, which allows them to deal with unforeseen problems swiftly and efficiently.

5.4 DWMs’ (data) practices

Before answering the last sub-question, an important difference has to be noted. There are three ways to create a market on the Dark Web, with each different purposes, advantages, and downsides. The first, and easiest way to sell illegal products on the Dark Web is by creating a store page on one of the already existing “eBay-like” DWMs. A few examples are Hydra, Alphabay, and the original Silk Road, where it is possible to rent a virtual spot to sell your goods. As this is merely renting a marketplace, it is not useful to this research.

The second option was to create your own DWM via a store builder called Deepify [24]. Deepify functioned the same way as Silk Road; they enabled other people to focus on selling their goods without having to worry about

the technical side of a DWM. The difference here is that Deepify store owners could use their own Onion link and customize their stores to a certain extent. However, after Deepify launched in May 2014, the site became inaccessible a short time later and got added to the deepdotweb directory of “dead” DWMs [25]. As this method is discontinued and most stores continued to sell their goods via a DWM like Silk Road, it is not possible to research Deepify. As an alternative is not available at the moment, creating a mock store via such a store builder is also not an option.

This leaves us with the third and most advanced option: creating a DWM like Silk Road where one’s own products are being sold, as well as hosting a marketplace for vendors to sell their goods. For this method, all the steps of the supply chain have to be tackled in order to create a successful business that can survive in this sector. Even though Silk Road, Alphabay and Hydra all use different methods, some core practices apply to all. The goal of this section is to find a common ground, and thus the practices that are customary for DWMs.

The configuration process of a DWM can be split up into three parts. First, the technical and legal aspects of setting up the server. This requires a decent amount of technical skill, as any minor mistake in this step of the process could lead to a gigantic leak further down the road. Nachash’s article [19] provides an overview of the initial steps that are required. After the website itself is configured, a supply chain has to be created as they need products to sell. An alternative to this step is to simply have vendors sell products, but the infrastructure of selling products through the website has to be configured regardless. Li et al.’s research [16] provides insight into the opioid supply chain, which will be the main source for this step. After the server, website, and products have been organized, the last step is to maintain all the aspects. This includes customer support, preventing external attacks to the website, and dealing with scamming vendors. In addition, Alphabay and Hydra can both be analysed to view how they tackle this step.

For the technical side, a good understanding of the Operating Software of choice and TOR is necessary. The returning motive is that one should want as much control as possible, the only exception being the hosting solution. This includes identifying pre-compiled software and compiling all the necessary applications yourself. By going to extreme lengths to figure out every detail about the server and applications, the only one fully in control, and to blame if anything goes wrong, is oneself. This methodology is applied by the largest DWMs in other aspects too. Trusting others can backfire with major consequences as a result, hence the tendency to keep control over every aspect of the business, even if this is not the most optimal or efficient approach. Another key takeaway from previous seizures of Alphabay and Silk Road is to be methodical and keep all the data secure. Alphabay got seized due to careless use of personal information, no encryption on the laptop used to run Alphabay, and using a personal Hotmail as the administrator [26].

The next step is to figure out a way to get products. As research by Li et al. has shown [16], there are a lot of major suppliers that are easy to track down via Dark Web forums. Due to the time constraint of this research, it was not possible to research the supply chain for other narcotics. However, given the availability of most drugs, it is highly probable that the same structure is set in place for other drugs. Another option is to directly hire chemists and growers to produce the products. This adds to the mo-

tive of keeping every aspect of the business under control. Hydra, for example, is actively hiring for such positions. The vacancies are available on their website. An example job advertisement can be seen in Figure 1, although the advertisement shown is for a narcolologist, an expert on drug abuse to assist drug addicts.

Figure 1. Example of a job advertisement on Hydra (translated from Russian)

Jobs at HYDRA
Narcological service HYDRA invites **narcologists** :

Requirements:

- Higher education in the specialty of general medicine, a valid certificate "narcology" "psychiatry-narcology", "psychotherapy"
- 3+ years of clinical experience
- Awareness in modern psychoactive substances, clinical pharmacology and their combination
- Experience in the treatment and rehabilitation of drug addicted patients
- Having a clinical mindset in psychiatry, addiction and emergency medicine
- Confident PC user

Duties:

- Strict adherence to work schedule
- Providing timely advice to drug addicts in matters related to PAS
- Monitoring the patient's condition during counseling and prescribing appropriate treatment
- Active dynamic monitoring of the patient's condition following the consultation
- Development of new treatment algorithms as experience gained in working with drug users

Conditions:

- Remote work
- Shift work schedule
- High profit payment
- Friendly professional team
- Trial period 2 months

Lastly, there is the maintenance of the DWM. From the technical maintenance of the website to offering support to customers. As the job vacancies in Hydra show, DWMs also create teams with specialists for each task. Hackers to maintain the server and counter external attacks, narcologists to assist drug addicts via forums and tickets, and couriers to hide the drugs for pick-up. The availability and steady supply of products is not perse an issue of the DWMs, as the vendors are mostly responsible for selling the goods. In addition, as research by Kilmer, Hoorens and RAND [15] has shown, the market of drugs functions as a free market; there is no governing body on the Dark Web. Thus, when one fails to deliver, space opens up for another to fill that supply gap. If this supply gap cannot be filled and the total supply drops, the prices will adjust accordingly.

6. DISCUSSION

The goal of this paper is to find useful DWM processes that can be applied to legitimate businesses. As the results show, there does not seem to be a defining DWM process that can be directly applied to businesses to improve them. However, there are three differences in methodology that could lead to improvements for legitimate businesses. These differences can be summarized in the following way.

First is the difference in the approach to data security between DWMs and legitimate businesses. While legitimate businesses seem to address data security to comply with the law as a necessity, DWMs address data security to protect themselves from complete seizure of their business. The increased risk and the lack of support of law enforcement, has forced DWMs to increase security to a higher standard than present by legitimate businesses. Any data leak can leave a trail back to the owner of the DWM. It is interesting to see that as a consequence, customers' data is in some cases better protected by an illegal online drug store, than by legal media companies. With further investigation into and practical testing of the security practices that are standard on the Dark Web, it could decrease the number of data breaches or leaks legitimate businesses suffer.

Another difference is the extreme lengths DWMs go to improve the customer's experience. Forums are being created, on-site cryptocurrency exchanges are being configured, and free of charge legal support is being offered to name a few examples. A lower price alone does not seem to attract customers; trust and safety are preferred. Although the anonymous nature of the Dark Web influences this preference, it might also be feasible for legitimate businesses. DWMs view customer support as an asset to win over customers, instead of viewing it as a necessity to handle problems with products. There is also a more proactive approach when it comes to the support a DWM offers, as this is one of the main selling points of their business. Customer support for a DWM is seen as a primary activity. It is interesting for legitimate businesses to look into adopting such a perspective for their customer support.

The last key difference is the amount of control that DWMs have over all the aspects of their business. Outsourcing, for example, is a commonly used method to reduce costs. However, this increases the risk of unforeseen problems. According to research by Somjai [27], outsourcing can even increase the risk of exposing confidential data and technology. In the long term, it might be more feasible to keep certain (technical) aspects of the business under its management. For a DWM, this control allows them to guarantee the security, privacy, and safety necessary for both themselves and their customers. Instead of the focus being on what is the most cost-effective, the focus is on security. This approach seems to pay off in the long run, as it increases customer satisfaction drastically.

7. CONCLUSION

In this paper, a methodology is described and executed to find practices or processes used by DWMs that could improve legitimate businesses. First, a baseline was set by comparing the DWMs to legitimate businesses and analysing the added challenges a DWM faces. Then a value chain analysis was performed on Hydra. This analysis, in addition to the research performed to find common DWMs' (data) practices, shows that there does not seem to be a defining DWM process that could improve legitimate businesses. However, this paper shows that the dark web environment forces DWMs to adopt better data security, control more aspects of the business, and increase customer service. This is expected by the customers of these DWMs, as the anonymous nature of the dark web requires DWMs to provide better safety and service in comparison to legitimate businesses. Thus, to have legitimate businesses adopt these improved practices, the customers of legitimate businesses must raise their expectations as well.

8. LIMITATIONS

Due to the time constraint of this research and the requirements to apply the methodology on a large scale, the theories and methods found have not yet been tested on legitimate businesses. Further research is required to see if the possible improvements mentioned in the conclusion are feasible. Due to the differences in environment between the dark web and the surface web, not all the suggestions are applicable. Nonetheless, this research does provide evidence that analysis of DWMs as businesses give an alternative perspective on existing problems.

In addition to the feasibility, the ethicality of the improvements should also be considered. As the DWMs covered in this research are illegal online markets, it is necessary to judge the ethics of any approach taken by these markets.

Lastly, Porter's value chain analysis was only applied to Hydra. Although Hydra is one of the largest DWMs currently, it cannot be seen as a representative for the DWMs as there are differences between Hydra and other major DWMs. While there is no set blueprint for a DWM supply chain, the analysis of more DWMs would give a clearer overview.

9. FUTURE WORK

For future work, it would be interesting to see the theories being put into practice and test what applies to legitimate businesses. Especially the security that DWMs offer through the extensive encryption which is also. To a certain extent, this would be possible on regular web browsers. If a regular webshop were to be configured with the same prioritization for certain aspects as a DWM, it could result in a webshop that sets new standards for privacy and safety.

Future research can also be performed on more DWMs, as the time constraint of this research caused the exclusion of several major DWMs. There might be useful practices used by these DWMs, that provide more insight or strengthen the theories in this research. This research is meant to be a mere start to the analysis of DWMs as a business.

10. REFERENCES

- [1] R. Dingledine, "The tor project: Privacy; freedom online," *Tor Project*, Mar 2011.
- [2] P. Syverson, "Onion routing," Jan 1998.
- [3] A. K. Jadoon, W. Iqbal, M. F. Amjad, H. Afzal, and Y. A. Bangash, "Forensic analysis of tor browser: A case study for privacy and anonymity on the web," *Forensic Science International*, vol. 299, pp. 59–73, 2019.
- [4] A. Gayathri, "From marijuana to lsd, now illegal drugs delivered on your doorstep," *International Business Times*, Nov 2011.
- [5] "United States of America v. Ulbricht, 13 CIV 6919," Sep 2013.
- [6] ACSI, "Acsi commentary july 2012," *American Customer Satisfaction Index*, Jul 2012.
- [7] B. Morgan, "Companies that failed at digital transformation and what we can learn from them," *Forbes*, Feb 2021.
- [8] Europol, "Darkmarket: world's largest illegal dark web marketplace taken down," Jan 2021.
- [9] Gwern, "Darknet market archives (2013–2015)," Dec 2013.
- [10] Команда «Проекта» (Team Project), "Вся эта дурь (all this nonsense)," Проект. (*Project*), Jul 2021.
- [11] N. R. Council, *Environmental Epidemiology, Volume 2: Use of the Gray Literature and Other Data in Environmental Epidemiology*. Washington, DC: The National Academies Press, 1997.
- [12] A. Zaunseder and A. Bancroft, "Pricing of illicit drugs on darknet markets: A conceptual exploration," *Drugs and Alcohol Today*, July 2020.
- [13] N. Christin, "Traveling the silk road: A measurement analysis of a large anonymous online marketplace," 2013.
- [14] D. Rhumorbarbe, L. Staehli, J. Broséus, Q. Rossy, and P. Esseiva, "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*, vol. 267, pp. 173–182, 2016.
- [15] B. Kilmer and e. Stijn Hoorens, "Understanding illicit drug markets, supply-reduction efforts, and drug-related crime in the european union," 2010.
- [16] Z. Li, X. Du, X. Liao, X. Jiang, and T. Champagne-Langabeer, "Demystifying the dark web opioid trade: Content analysis on anonymous market listings and forum posts," *J Med Internet Res*, vol. 23, p. e24486, Feb 2021.
- [17] J. Bartlett, "Dark net markets: The ebay of drug dealing," *The Guardian*, Oct 2014.
- [18] T. Fox-Brewster, "The darkweb's nihilistic vigilante sees the light," Dec 2014.
- [19] Nachash, "So, you want to be a darknet drug lord," Jan 2016.
- [20] A. S. Babrahem, E. T. Alharbi, A. M. Alshiky, S. S. Alqurashi, and J. Kar, "Study of the security enhancements in various e-mail systems," *Journal of Information Security*, vol. 06, no. 01, p. 1–11, 2015.
- [21] A. Reuter, A. Abdelmaksoud, K. Boudaoud, and M. Winckler, "Usability of end-to-end encryption in e-mail communication," *Frontiers in Big Data*, vol. 4, p. 42, 2021.
- [22] I. Ladegaard, "Instantly hooked? freebies and samples of opioids, cannabis, mdma, and other drugs in an illicit e-commerce market," *Journal of*

- Drug Issues*, vol. 48, no. 2, pp. 226–245, 2018.
- [23] M. Tzanetakis, G. Kamphausen, B. Werse, and R. von Laufenberg, “The transparency paradox. building trust, resolving disputes and optimising logistics on conventional and online drugs markets,” *The International journal on drug policy*, vol. 35, 12 2015.
 - [24] P. H. O’Neill, “Deepify lets you make your own deep web black market in 60 seconds,” *The Daily Dot*, Mar 2014.
 - [25] DeepDotWeb, “Dead/scam,” *Marketplace directory of Dead/Scam marketplaces*, Apr 2015.
 - [26] K. McCarthy, “Alphabay shutdown: Bad boys, bad boys, what you gonna do? not use your hotmail...,” *The Register - Biting the hand that feeds IT*, Jul 2017.
 - [27] S. Somjai, “Advantages and disadvantages of outsourcing,” *The Business and Management Review*, vol. 9, no. 1, pp. 157–160, 2017.