The Dark Web: A Brief Introduction

Soldner, Felix

Empfohlene Zitierung / Suggested Citation:
Soldner, F. (2023). The Dark Web: A Brief Introduction. *easy_social_sciences*, 69, 18-27. https://doi.org/10.15464/easy.2023.09

easy_social_sciences 69 ▪ 2023 | doi: 10.15464/easy.2023.09

The Dark Web

A Brief Introduction

Felix Soldner

The dark web is a highly anonymized section of the Internet in which some users share sensitive and illicit content. Users on the dark web generate digital traces, allowing researchers to study previously difficult-to-observe phenomena, such as trading illegal products or services. Trading occurs on darknet markets, platforms that provide the infrastructure for vendors and buyers to convene, similar to surface web platforms, such as eBay. Listings on such markets predominantly include drugs but also fraud items, counterfeits, or cybercrime-related services, such as hacking. Studying the dark web can be challenging due to technical and ethical considerations. This article introduces the dark web and Tor, the most prominent used dark web network. The article continues with a brief overview of how users engage with the dark web and darknet markets and discusses past research as well as possible future avenues for further research.

*Das Dark Web ist ein stark anonymisierter Teil des Internets, in dem einige Nutzer*innen sensible und illegale Inhalte teilen. Sie hinterlassen dabei digitale Spuren, die es Forscher*innen ermöglichen, zuvor schwer zu beobachtende Phänomene zu untersuchen, wie zum Beispiel das Handeln mit illegalen Produkten oder Dienstleistungen. Solcher Handel findet auf Darknet-Märkten statt, Plattformen, die ähnlich wie etwa eBay eine Infrastruktur für Käufer*innen und Verkäufer*innen bereitstellen. Die Angebote auf solchen Märkten umfassen überwiegend Drogen, beinhalten aber auch Fälschungen, Betrugsanleitungen oder kriminelle Dienstleistungen wie Hacking Attacken. Allerdings wird die wissenschaftliche Erforschung des Dark Webs oft durch technische und ethische Hürden erschwert. Dieser Artikel stellt das Dark Web vor und erläutert die Funktionsweise von Tor, dem am häufigsten genutzte Dark-Web-Netzwerk. Darüber hinaus wird erklärt, wie Darknet-Märkte operieren und wie diese genutzt werden. Abschließend werden mögliche Forschungsrichtungen, sowie rechtlich und ethische Probleme diskutiert.*

Keywords: darknet markets, crypto markets, tor network

The dark web is often imagined as an outlandish section of the Internet and mentioned in the context of illegal activity, such as drug trading, hacking, or contract killings. Since the dark web anonymizes user activity on the Internet, it is also called an anonymous network, which is used for illicit trading and enables users to overcome governmental censorship and communicate more securely. Thus, investigating such anonymized networks is worthwhile for a broad range of researchers that are not only interested in crime-related behavior (e.g., drug usage, fraud, hacking) but also in wider societal phenomena, such as extremism, political attitudes, organized movements (e.g., protests), whistleblowing, or conspiratorial beliefs.

After providing a basic understanding of

the dark web, followed by explanations of darknet markets (platforms used to trade goods and services), I will illustrate how such markets operate, and how users interact with them.

What is the Dark Web?

The *dark web* describes a section of the Internet in which the communication between computers differs from the Internet we use daily. The "everyday" Internet with which we primarily interact is also called the surface web (see Figure 1) and includes websites, such as news sites or shopping platforms, that are accessible with traditional browsers (e.g., Chrome, Firefox) and are indexed by search engines (e.g., Google, Bing, DuckDuckGo). In contrast, online content that is protected through barriers, hidden from the public, and not indexed by search engines is considered part of the so-called deep web (Figure 1). The deep web includes personal cloud storage (e.g., Dropbox, OneDrive), paywalled content (e.g., streaming services), or databases. Communications between computers on the surface and deep web are identifiable through their Internet Protocol (IP) address and unique *cookie* settings[1]. In most cases, communication between computers is recorded and stored, making our online behavior visible to others, often resulting in tracking and targeted actions, such as personalized advertisements.

The *dark web* can be regarded as a small sub-part of the *deep web* (Figure 1), on which the communication between computers is anonymized, thus, also called an anonymized network (Gehl, 2018; Ghosh et al., 2017; Mansfield-Devine, 2009). The Tor network is the most known access point to such a *network*, but other technologies can also facilitate anonymity, such as the

The deep web is considered the largest and fastest-growing part of the Internet.

Invisibility Internet Project (I2P) or *Freenet* (Gehl, 2018). These technologies provide anonymity by sending the computers' encrypted communication through a network that conceals the true IP address. The Tor, I2P, or Freenet networks can be accessed through standard web browser technology. (The Tor client is built onto Firefox and can be downloaded *here*.) Accessing websites on such networks requires exact addresses since the software facilitating the creation of the network prevents classical search engines from finding and indexing websites on the network. However, lists of websites exist and are published on forums or websites, such as *reddit.com*, *thehiddenwiki.org*, or *dark.fail*.

Making size comparisons between the different parts of the Internet is difficult due to the unindexed content of the anonymized networks. Currently (January 16th, 2023), the surface web seems to contain over 1,1 billion websites (Netcraft, 2023), while only 18% of them contain and load content (Huss, 2022). Thus, most websites seem to be inactive or unused. Estimations about the number of dark web sites on the Tor network vary considerably but are thought to be much lower than on the surface web. While past investigations found

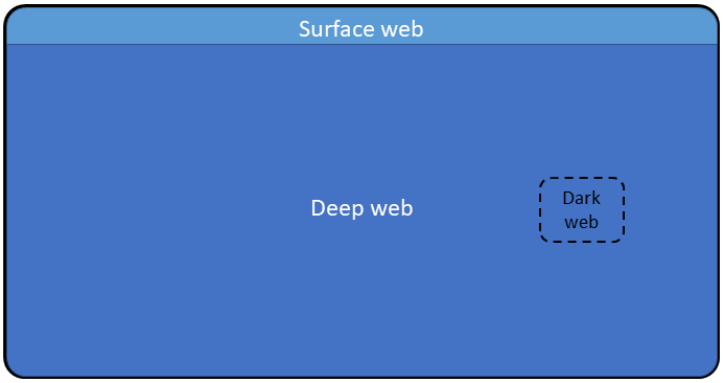

Figure 1 The Internet can be subdivided into the surface, deep, and dark web. The proportions of each part are rough approximations for illustration purposes; figure from (Soldner et al., 2022).

1 Saved websites & user settings.

around 32,000 sites on the Tor network, fewer than half of those seem active (Ghosh et al., 2017; Gray, 2019; Lewis, 2017). By contrast, the deep web is considered the largest and fastest-growing part of the Internet, with some estimating it to contain 400-500 times more data (i.e., stored information) than the surface web (Bergman, 2001; He et al., 2007).

The Tor Network

Tor (**T**he **O**nion **R**outing) uses *onion routing* to protect the user's privacy and was created by the US Naval Research Laboratory in the mid-1990s (Syverson, 2005; The Tor Project, Inc., 2020). Onion routing entails encrypting and relaying messages from the client (i.e., user) to a server, thereby anonymizing the user's internet activity. Tor uses three random relays that forward the messages from the client to the server (Figure 2).

Each relay provides an encryption layer that will either decrypt (when the client sends a message to the server) or encrypt (when the server sends a message to the client) the message with its encryption key (K). Multiple encryption keys are held by the client (who can decrypt and encrypt all messages) and by the individual relays. For example, the message is encrypted multiple times when the client wants to visit a website (i.e., sending a message to a server) through the Tor network. The first relay can decrypt the first layer of encryption, the second relay the second, and so forth. Thus, like layers in an onion, the relays decrypt each layer with a decryption key, hence the term "onion routing". Similarly, messages can be encrypted multiple times when sent from the server to the client, which can then decrypt all layers.

Since Tor relies on a decentralized network, more computers using the software create more *relays* (also called *nodes*) through which the network traffic is sent. A more extensive network facilitates a more secure space since more relays can be utilized, making tracking more difficult. To expand the decentralized network, Tor was released to the public in 2002 (Syverson, 2005; The Tor Project, Inc., 2020). The Tor project became a nonprofit organization in 2006. From 2007 onwards, changes were implemented to allow users to access the open web, circumventing censorship, for which the Tor browser is often used today. Those implementations can overcome local internet restrictions for specific countries (e.g., Russia, China). However, visiting surface websites with Tor is less anonymous than visiting sites within the Tor network, which is why some US governmental agencies (e.g., CIA, FBI), as well as other organizations (e.g., BBC, The New York Times, Facebook), also operate websites on the Tor network. Websites on the Tor network are also called "onion sites", and their administrative markers or country codes, such as ".de" or ".com", are replaced by the top-level domain ".onion".

Due to the anonymous and secure communication provided by Tor, the network is valuable for individuals who want to share sensitive information and want to protect their identity (e.g., journalists, whistleblowers). Similarly,

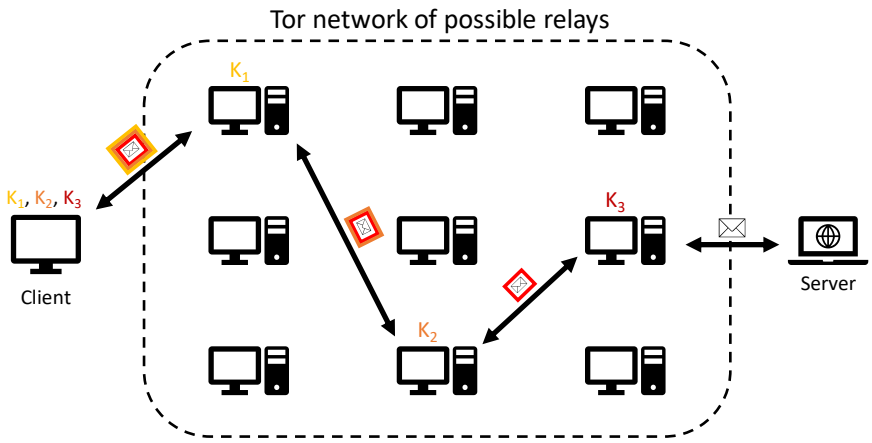

Figure 2 Visualization of how messages are sent from a client to a server through the Tor network; adapted from The Tor Project, Inc. (2020).

individuals use Tor to circumvent internet restrictions (often imposed by authoritarian regimes) and prevent tracking by state or industry actors. However, the Tor network is also used for illicit trading, including drugs, stolen goods, or digital items and services (e.g., hacking services). Trades of illicit goods are often carried out on darknet markets, which provide an infrastructure where users can transact goods and services with each other, similar to the surface web platform eBay. The Tor network, on which many markets exist, will be the focus for the remainder of this text due to its relatively widespread and larger-scale usage compared to other networks.

What are Darknet Markets?

At the beginning of 2011, the infamous online market "Silk Road" started operating on the Tor network, offering many illicit goods, predominantly drugs (e.g., cannabis, ecstasy, opioids), but also digital goods (e.g., hacking guides), apparel, electronics and more (Christin, 2013). In late 2013, the alleged site operator, Ross Ulbricht, was arrested, and US authorities shut the market down (CNN, 2013; EMCDDA-Europol, 2017). Around one month after the closure, Silk Road 2.0 was launched next to many similar sites (e.g., Pandora, Sheep Marketplace, BuyItNow). Since then, dark markets have been abundantly present on the network, but many operate only for a few months due to low traffic, voluntary closures, authority interventions, or "exit scams"[2] (EMCDDA-Europol, 2017).

Darknet markets, also called "black markets" or "crypto markets", mainly use cryptocurrencies for monetary exchanges, further supporting user anonymity, which is explained in more detail below. Some specialized markets offer only one product type, such as cannabis or stolen credit card information (Marin et al., 2016; Soska & Christin, 2015). Others are more general and offer a range of products, including fake documents (e.g., Passports), counterfeits (e.g., money, clothes), or firearms (Baravalle & Lee, 2018). Figure 3 provides an example of a listing on the market "Darkode". Sellers often customize offers for specific buyers, which can be arranged through chats, and name the listings "custom listing for [Username]".

Furthermore, markets often self-impose rules on what can be offered and sold. Next to general and specialized markets, more exclusive markets are also present, which are only accessible through invitations. However, invitations can sometimes be bought on other markets. While marketplaces are currently the predominant sales platforms, more shops are emerging that offer goods from a single seller, resembling retailer platforms (Oosthoek et al., 2023).

Accessing and browsing darknet markets often requires registration. Beyond having to solve unusually difficult Captchas, creating an account resembles registrations on surface web platforms. However, further interactions (e.g., posting, chatting, purchasing) mostly require *PGP keys* (Pretty Good Privacy), which encrypt messages and enable secure communications between users (Ailipoaie & Shortis, 2015). Each user requires a public and private PGP key for this encryption technology. For example, if a customer wants to send a message to a vendor, the customer uses the vendor's public key (often available on the vendor's profile) to encrypt a message. The message is then sent to the vendor, who can decrypt the message with their private key. In short, public keys are available to everyone to encrypt messages, while the private key is only known to the message receiver and is used to decrypt messages (For more details on PGP see: *openpgp.org*). Since vendors operate across platforms, PGP keys are also used as an identity verification tool (Ailipoaie & Shortis, 2015).

Payments on crypto markets are handled through *cryptocurrencies* (e.g., Bitcoin, Ethereum), which can be acquired through online exchanges, such as *Coinbase*, *Bitstamp*, or

2 A scam in which all the monetary user funds stored with the market website are stolen by hackers or the operators of the website, resulting in a closure.

direct transfers from other individuals. Cryptocurrencies are decentralized, anonymous, and rely on a peer-to-peer system, circumventing a governing third party, such as a bank (Rickens, 2019). The currencies can be held online on exchanges, the markets, or a local machine. Storing the currency locally with software is often preferred since it reduces the risk of theft through exit scams or hacks (EMCDDA-Europol, 2017). Since many cryptocurrency exchanges do not require personal information for registrations, the users' true identities often remain unknown. Further currency laundering through online *mixers* (*tumblers*)[3] makes the transactions virtually anonymous, complicating tracking for law enforcement (Europol, 2021; Möser et al., 2013). Thus, combining the Tor network and cryptocurrencies enables a highly anonymous environment for communication and trading.

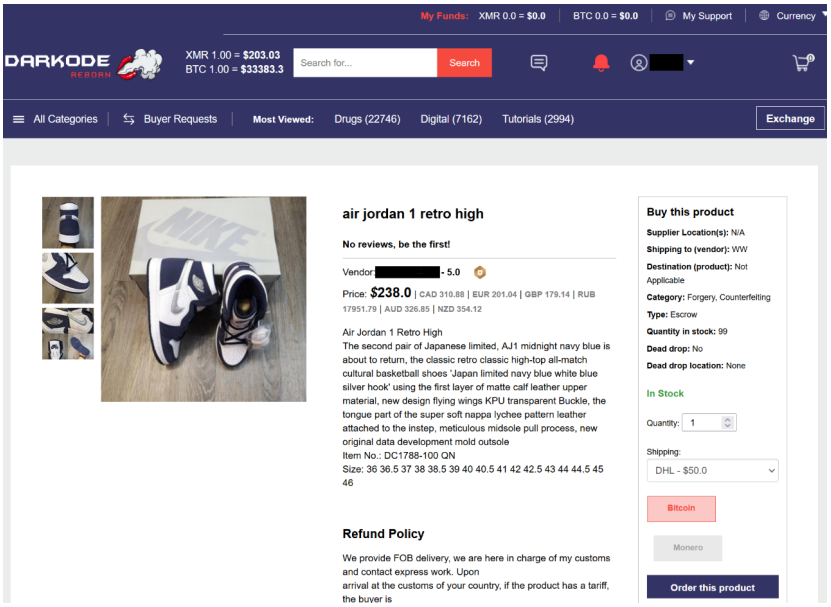

Figure 3 Screenshot of a counterfeit (Air Jordan shoes) sold on the darknet market "Darkode" on the Tor network.

The minimal oversight on cryptomarkets makes both customers and vendors vulnerable to fraud, such as sending payments without receiving the product or vice versa. To curb fraud, markets often implement escrow systems, mostly integrated within the markets. Buyers who want to make a purchase deposit the required funds into the escrow system. These funds are withheld until the buyer receives the product, allowing for a more secure transaction. Market operators often take commissions through escrow and oversee transactions (Christin, 2013). Large funds held in the markets owned escrow system are also believed to have led to past exit scams (EMCDDA-Europol, 2017).

Why and How to Research the Dark Web?

The dark web has mostly been researched within security-related disciplines and computer science. For example, researchers have examined the infrastructures of the dark web, tested potential security issues (e.g., how well communications are kept anonymous), or developed new encryption methods (Alidoost Nia & Ruiz-Martínez, 2018; Alsabah & Goldberg, 2016). An extensive overview of such security and encryption research is provided by Huete Trujillo & Ruiz-Martínez (2021). At the same time, recent years have seen increased research on crypto markets, forums, and their users, but mostly with quantitative approaches (Gehl, 2018). Fewer researchers investigate users' behavior, motivations, and opinions on dark web platforms qualitatively through observations or interviews (Barratt et al., 2016; Barratt & Maddox, 2016). Since many researchers take a quantitative approach, some research attention has shifted to automated large-scale data collection methods (Ball et al., 2019; Yannikos et al., 2022). Collecting data automatically from the dark web is difficult due to the long loading times of

3 For more details on Tumblers see: Möser et al. (2013).

the websites (due to the many relays through the network) and implemented security features (e.g., advanced Captchas, extended registration procedures) or anti-crawling measures (e.g., detection of fast navigation behavior on the website) (Georgoulias et al., 2021). Data collection is further complicated by the uniqueness of the websites, requiring custom-made scrapers (programs that automatically collect web data) for almost every website. Because of these difficulties, incomplete data is a common issue, and automated solutions can be unreliable (Munksgaard et al., 2016), which led some to argue that manual collection approaches should be preferred to ensure adequate data quality (Van Buskirk et al., 2014, 2015).[4]

According to past research, the earliest known market, the Farmer's Market, seemed to have started operating in 2010 and closed in 2012 (EMCDDA-Europol, 2017). The Silk Road 1 closely followed (2011-2012), which was the first platform to receive more in-depth scholarly attention, followed by many more market openings. Silk Road 1 contained around 220 product categories, and Christin (2013) estimated that it harbored around 30,000-150,000 customers, with vendors generating a monthly revenue of around $1.2 million in 2012. Later studies also focused on single big markets, such as Alphabay (Baravalle & Lee, 2018) or Hydra (Goonetilleke et al., 2022). Alphabay was one of the biggest markets at its time (2015-2017), with estimated sales values of $79.8 million over the two years. Drugs were the predominant listings of the market, contributing around $69.2 million to all sales on the market, while other products, such as fraud-related items (e.g., guides), counterfeits, or services (e.g., hacking) were also present (Baravalle & Lee, 2018). Hydra, operated from 2015 to 2022, grew bigger than Alphabay and was estimated to account for around $5 billion in transactional value over its lifespan (Goonetilleke et al., 2022). Drugs were also the predominant product category, but unlike other markets, it also implemented drop-offs (products were dropped at hidden locations where buyers could collect them from after the purchase) as an alternative to postal deliveries to circumvent authority inspections, which seemed to be one of the reasons for the market's success.

Other cryptomarket studies expanded to include multiple markets in an attempt to estimate the scale of the entire dark web economy, both in general and for specific product categories, such as COVID-19-related products (e.g., masks, vaccines, personal protective equipment) (Bracci et al., 2022; Oosthoek et al., 2023; Soska & Christin, 2015). For example, Soska & Christin (2015) collected data on 35 markets between 2013 and 2015 and estimated an accumulated peak daily sales volume of up to $600,000 in mid-2014, and over 9,000 sellers were estimated to be operating across markets. Estimating sales volumes can be challenging and is often achieved through counting unique reviews. Buyer feedback through reviews is very important in crypto markets due to the lack of vendor verifications (Batikas & Kretschmer, 2018; Tzanetakis et al., 2016).

Since the dark web is highly anonymized, estimating unique vendors can also be complicated but is often achieved through PGP-key identifications or comparisons of image or text styles from product listings (Ho & Ng, 2016; Wang, 2018). Studying crypto markets, specifically, their products and services, allows researchers to better understand the economic breadth of illicit markets that were difficult to observe previously. Thus, helping to understand the possible impact of specific products or services, their demand, and availability. Most research concerns drug market behavior, but fraud or hacking-related offers are investigated as well. For example, previous studies examined fraud and hacking-related services, including the registration of fake businesses, the procurement of airplane tickets, or the capabilities of denial-of-service attacks (Hutchings, 2018; Hyslip & Holt, 2019). Examining how such services are used and implemented helps us understand how to protect against or

4 Some open available data can be found here: https://gwern.net/DNM-archives (Branwen et al., 2015).

deal with them. However, crypto markets also allow researchers to examine user interactions and behaviors to better understand their attitudes and motivations. Drug user behavior is most prominent, but trust building, accountability, advertising, and other vendor or buyer behaviors can also be studied.

Since market closures are common, researchers have investigated the effects of market disruptions on vendor and buyer migrations, vendor resilience across platforms, and offline crime (Décary-Hétu & Giommoni, 2017; ElBahrawy et al., 2020; Zambiasi, 2022). Some research has found that market closures due to authority interventions or other reasons seem to have limited effects, with buyers and sellers adapting and migrating to other markets quickly. Prices seem stable even after market shutdowns, and larger vendors, often present on multiple markets, show stronger resilience than smaller vendors (Décary-Hétu & Giommoni, 2017; ElBahrawy et al., 2020). There is also evidence that offline drug sales seem to increase shortly after big market closures but quickly drop to pre-closure levels (Zambiasi, 2022). However, intervention or disruption approaches to reduce crime-related activity in crypto markets are not well studied, with some research examining warning messages or rumor spreads as alternatives to market shutdowns (Howell et al., 2022; Hutchings & Holt, 2017).

Research Challenges and Ethical Considerations

Due to the challenges associated with collecting data from anonymous networks, large-scale analyses are not as abundant, and data is scarce. Contributing to data collection approaches and extending existing data repositories are still open issues that could be addressed by making methods and data more readily available. Such data scarcity is further exacerbated for anonymous networks other than Tor and market dissimilar

Researchers could explore differences in user behavior, including research on political opinions, conspiracy beliefs, or extremism.

platforms, such as forums. With such data, researchers could explore differences in user behavior across anonymized and surface web platforms, including research on political opinions, conspiracy beliefs, or extremism.

Cryptomarkets often have associated forums that could be linked with listing data to better understand the behavior and motivations of vendors and users. For example, understanding why and how cybercrime-related services are used (e.g., for misinformation campaigns) could facilitate better implementations of preventative measures. Furthermore, examining whether and how political movements utilize anonymous networks could be interesting.

Research around anonymous networks, specifically crypto markets, is often faced with legal and ethical considerations that are not always easy to address, along with common issues such as data protection. Notably, depending on the level of engagement from the researchers (e.g., observations, survey), the legal and ethical situation can become complicated quickly. For example, many institutional ethical guidelines recommend that researchers inform potential participants about their study and intentions, which collides with the principle of most users not to share personal information on anonymous networks (Gehl, 2018). Sharing personal information from and about the researchers has led at least once to threats and abuse to the investigators in the past (Martin & Christin, 2016).

However, conducting observational studies can also bring challenges. For example, collecting data on illegal products onto a local machine may be unlawful. Furthermore, ethical considerations may differ for users on anonymous networks, depending on their roles (e.g., site administrators, vendors, and

consumers) (Martin & Christin, 2016). As an example, estimating sales volumes for specific vendors could – in theory – be used against them if they were brought to trial. Further information around legal issues (e.g., when to report a possible crime) for the German context can be found in (RatSWD, 2023). Although essential to reproducibility, publicly sharing data is even more complicated as it may contain personal identifiable information, potentially harming users, especially in illegal contexts. The previous considerations only briefly touch on some key ethical considerations; the interested reader can look at the more in-depth discussion of these issues by Martin and Christin (2016).[5]

Technical and Legal Hurdles Complicate Dark Web Research

This paper introduced the dark web (anonymous networks), such as Tor and crypto market research, and provided starting resources for anyone interested in researching this space. Since users openly share sensitive information and conduct illicit businesses on anonymous networks, such spaces allow researchers to examine previously difficult-to-observe phenomena. However, anonymous networks are still understudied, especially outside of market environments. Technical and ethical hurdles surrounding collecting and sharing data from such networks are notable barriers. To address those barriers, collection methods and data should be shared more openly and documented to enable or facilitate reuse.

5 Some of the cited studies in this paper also include ethical or legal assessments related to their research (Barratt et al., 2016; Barratt & Maddox, 2016; Christin, 2013; Gehl, 2018; Soska & Christin, 2015).

References

Ailipoaie, A., & Shortis, P. (2015). *From Dealer to Doorstep – How Drugs Are Sold On the Dark Net.* Global Drugs Policy Observatory.

Alidoost Nia, M., & Ruiz-Martínez, A. (2018). Systematic literature review on the state of the art and future research work in anonymous communications systems. *Computers & Electrical Engineering, 69*, 497–520. https://doi.org/10.1016/j.compeleceng.2017.11.027

Alsabah, M., & Goldberg, I. (2016). Performance and Security Improvements for Tor: A Survey. *ACM Computing Surveys, 49*(2), 32:1-32:36. https://doi.org/10.1145/2946802

Ball, M., Broadhurst, R., Niven, A., & Trivedi, H. (2019). *Data Capture and Analysis of Darknet Markets.* 15.

Baravalle, A., & Lee, S. W. (2018). Dark Web Markets: Turning the Lights on AlphaBay. In H. Hacid, W. Cellary, H. Wang, H.-Y. Paik, & R. Zhou (Eds.), *Web Information Systems Engineering – WISE 2018* (Vol. 11234, pp. 502–514). Springer International Publishing. http://link.springer.com/10.1007/978-3-030-02925-8_35

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

Barratt, M. J., & Maddox, A. (2016). Active engagement with stigmatised communities through digital ethnography. *Qualitative Research, 16*(6), 701–719. https://doi.org/10.1177/1468794116648766

Batikas, M., & Kretschmer, T. (2018). Entrepreneurs on the Darknet: Reaction to Negative Feedback. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3238141

Bergman, M. K. (2001). White Paper: The Deep Web: Surfacing Hidden Value. *Journal of Electronic Publishing, 7*(1). http://dx.doi.org/10.3998/3336451.0007.104

Bracci, A., Nadini, M., Aliapoulios, M., McCoy, D., Gray, I., Teytelboym, A., Gallo, A., & Baronchelli, A. (2022). Vaccines and more: The response of Dark Web marketplaces to the ongoing COVID-19 pandemic. *PLOS ONE, 17*(11), e0275288. https://doi.org/10.1371/journal.pone.0275288

Branwen, G., Christin, N., Décary-Hétu, D., Andersen, R. M., StExo, El Presidente, Anonymous, Lau, D., Sohhlz, Kratunov, D., Cakic, V., Whom, McKenna, M., & Goode, S. (2015). *Dark Net Market archives, 2011-2015* (2015-07-12). https://www.gwern.net/DNM-archives

Christin, N. (2013). Traveling the silk road: A measurement analysis of a large anonymous online marketplace. *Proceedings of the 22nd International Conference on World Wide Web - WWW '13*, 213–224. https://doi.org/10.1145/2488388.2488408

CNN, B. T. H. (2013, October 5th). *How the FBI caught Ross Ulbricht, alleged creator of Silk Road*. CNN. https://www.cnn.com/2013/10/04/world/americas/silk-road-ross-ulbricht/index.html

Décary-Hétu, D., & Giommoni, L. (2017). Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous. *Crime, Law and Social Change, 67*(1), 55–75. https://doi.org/10.1007/s10611-016-9644-4

ElBahrawy, A., Alessandretti, L., Rusnac, L., Goldsmith, D., Teytelboym, A., & Baronchelli, A. (2020). Collective dynamics of dark web marketplaces. *Scientific Reports, 10*(1), 18827. https://doi.org/10.1038/s41598-020-74416-y

EMCDDA-Europol. (2017). *Drugs and the darknet: Perspectives for enforcement, research and policy*. Publications Office of the European Union.

Europol. (2021). *Cryptocurrencies: Tracing the evolution of criminal finances*. Publications Office of the European Union. https://data.europa.eu/doi/10.2813/75468

Gehl, R. W. (2018). Archives for the Dark Web: A Field Guide for Study. In lewis levenberg, T. Neilson, & D. Rheams (Eds.), *Research Methods for the Digital Humanities* (pp. 31–51). Springer International Publishing. https://doi.org/10.1007/978-3-319-96713-4_3

Georgoulias, D., Pedersen, J. M., Falch, M., & Vasilomanolakis, E. (2021). A qualitative mapping of Darkweb marketplaces. *2021 APWG Symposium on Electronic Crime Research (ECrime)*, 1–15. https://doi.org/10.1109/eCrime54498.2021.9738766

Ghosh, S., Porras, P., Yegneswaran, V., Nitz, K., & Das, A. (2017). ATOL: A Framework for Automated Analysis and Categorisation of the Darkweb Ecosystem. In *Workshops at the Thirty-First AAAI Conference on Artificial Intelligence*.

Goonetilleke, P., Knorre, A., & Kuriksha, A. (2022). Hydra: A Quantitative Overview of the World's Largest Darknet Market. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4161975

Gray, H. (2019). *Dark Web Map*. https://www.hyperiongray.com/dark-web-map/#zoom=0.8521016982969332&x=0.5064520330563047&y=0.572866049039204

He, B., Patel, M., Zhang, Z., & Chang, K. C.-C. (2007). Accessing the deep web. *Communications of the ACM, 50*(5), 94–101. https://doi.org/10.1145/1230819.1241670

Ho, T. N., & Ng, W. K. (2016). Application of Stylometry to DarkWeb Forum User Identification. In K.-Y. Lam, C.-H. Chi, & S. Qing (Eds.), *Information and Communications Security* (Vol. 9977, pp. 173–183). Springer International Publishing. https://doi.org/10.1007/978-3-319-50011-9_14

Howell, C. J., Maimon, D., Perkins, R. C., Burruss, G. W., Ouellet, M., & Wu, Y. (2022). Risk Avoidance Behavior on Darknet Marketplaces. *Crime & Delinquency,* 00111287221092713. https://doi.org/10.1177/00111287221092713

Huete Trujillo, D. L., & Ruiz-Martínez, A. (2021). Tor Hidden Services: A Systematic Literature Review. *Journal of Cybersecurity and Privacy, 1*(3), Article 3. https://doi.org/10.3390/jcp1030025

Huss, N. (2022, April 6). How Many Websites Are There in the World? (2023). *Siteefy*. https://siteefy.com/how-many-websites-are-there/

Hutchings, A. (2018). Leaving on a jet plane: The trade in fraudulently obtained airline tickets. *Crime, Law and Social Change, 70*(4), 461–487. https://doi.org/10.1007/s10611-018-9777-8

Hutchings, A., & Holt, T. J. (2017). The online stolen data market: Disruption and intervention approaches. *Global Crime, 18*(1), 11–30. https://doi.org/10.1080/17440572.2016.1197123

Hyslip, T. S., & Holt, T. J. (2019). Assessing the Capacity of DRDoS-For-Hire Services in Cybercrime Markets. *Deviant Behavior, 40*(12), 1609–1625. https://doi.org/10.1080/01639625.2019.1616489

Lewis, S., Jamie. (2017, March 6th). *OnionScan Report: Freedom Hosting II, A New Map and a New Direction*. Mascherari Press. https://mascherari.press/onionscan-report-fhii-a-new-map-and-the-future/

Mansfield-Devine, S. (2009). Darknets. *Computer Fraud & Security, 2009*(12), 4–6. https://doi.org/10.1016/S1361-3723(09)70150-2

Marin, E., Diab, A., & Shakarian, P. (2016). Product Offerings in Malicious Hacker Markets. *ArXiv:1607.07903 [Cs]*. http://arxiv.org/abs/1607.07903

Martin, J., & Christin, N. (2016). Ethics in cryptomarket research. *International Journal of Drug Policy, 35*, 84–91. https://doi.org/10.1016/j.drugpo.2016.05.006

Möser, M., Böhme, R., & Breuker, D. (2013). An inquiry into money laundering tools in the Bitcoin ecosystem. *2013 APWG ECrime Researchers Summit*, 1–14. https://doi.org/10.1109/eCRS.2013.6805780

Munksgaard, R., Demant, J., & Branwen, G. (2016). A replication and methodological critique of the study "Evaluating drug trafficking on the Tor Network." *International Journal of Drug Policy, 35*, 92–96. https://doi.org/10.1016/j.drugpo.2016.02.027

Netcraft. (2023, January 16th). *Web Server Survey*. Netcraft News. https://news.netcraft.com/archives/category/web-server-survey/

Oosthoek, K., Van Staalduinen, M., & Smaragdakis, G. (2023). Quantifying Dark Web Shops' Illicit Revenue. *IEEE Access, 11*, 4794–4808. https://doi.org/10.1109/ACCESS.2023.3235409

RatSWD. (2023). Handreichung Umgang mit der Kenntnisnahme von Straftaten im Rahmen der Durchführung von Forschungsvorhaben. *RatSWD Output Paper Series*. https://doi.org/10.17620/02671.74

Rickens, E. (2019). *What Are Cryptocurrencies: The Basics*. https://blog.blockport.io/what-are-cryptocurrencies/

Soldner, F., Kleinberg, B., & Johnson, S. (2022). Trends in online consumer fraud: A data science perspective. In *A Fresh Look at Fraud*. Routledge.

Soska, K., & Christin, N. (2015). Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem. *Proceedings of the 24th USENIX Security Symposium*, 33–48.

Syverson, P. (2005). *Onion Routing*. https://www.onion-router.net/

The Tor Project, Inc. (2020). *The Tor Project | Privacy & Freedom Online*. https://torproject.org

Tzanetakis, M., Kamphausen, G., Werse, B., & von Laufenberg, R. (2016). The transparency paradox. Building trust, resolving disputes and optimising logistics on conventional and online drugs markets. *International Journal of Drug Policy, 35*, 58–68. https://doi.org/10.1016/j.drugpo.2015.12.010

Van Buskirk, J., Roxburgh, A., Farrell, M., & Burns, L. (2014). The closure of the Silk Road: What has this meant for online drug trading?: Editorial. *Addiction, 109*(4), 517–518. https://doi.org/10.1111/add.12422

Van Buskirk, J., Roxburgh, A., Naicker, S., & Burns, L. (2015). A response to Dolliver's "Evaluating drug trafficking on the Tor network." *International Journal of Drug Policy, 26*(11), 1126–1127. https://doi.org/10.1016/j.drugpo.2015.07.001

Wang, X. (2018). *Photo-based Vendor Re-identification on Darknet Marketplaces using Deep Neural Networks* [Master Thesis]. Faculty of the Virginia Polytechnic Institute and State University.

Yannikos, Y., Heeger, J., & Steinebach, M. (2022). Data Acquisition on a Large Darknet Marketplace. *Proceedings of the 17th International Conference on Availability, Reliability and Security*, 1–6. https://doi.org/10.1145/3538969.3544472

Zambiasi, D. (2022). Drugs on the Web, Crime in the Streets. The Impact of Shutdowns of Dark Net Marketplaces on Street Crime. *Journal of Economic Behavior & Organization, 202*, 274–306. https://doi.org/10.1016/j.jebo.2022.08.008

Felix Soldner

GESIS – Leibniz Institute for the Social Science, Köln, Germany

Dawes Centre for Future Crime, Department of Security and Crime Science, University College London, UK

E-Mail felix.soldner@gesis.org

Felix Soldner arbeitet als wissenschaftlicher Mitarbeiter bei GESIS im Department Computational Social Science. Seine Forschung umfasst Themen wie online Betrug, Cryptomärkte, Täuschungserkennung und Datenverzerrungen. Dabei interessieren ihn die Nutzung von Methoden in Bereichen von Natural Language Processing (NLP) und maschinelles Lernen.