Decentral, unbreakable and anonymous?

Literature Review of resiliency mechanisms in darknet markets

Bjoern Christian Wolf
MSc in Information Systems and Digital Innovation
Department of Management
London School of Economics and Political Science

KEYWORDS

Cybercrime
Cryptomarkets
Drug distribution networks
Market mechanisms
Spontaneous order

ABSTRACT

This article identifies socio-technical mechanisms of darknet markets that render them resilient to law enforcement based on relevant literature. In depth, it analyses the interplay between user or community behaviour and cryptographic technology. The four main activities of darknet markets that are necessary for successful coordination are identified as: (1) transaction and communication, (2) trust and reputation, (3) payment and (4) logistics, each addressed through a combination of ICTs and community norms. The marketplaces act as intermediaries facilitating an anonymous, decentralised market by joining these four areas and offering a resilient solution.

Introduction

After the advent (and demise) of Silk Road, the first online market for drugs and other illegal goods, darknet marketplaces or cryptomarkets have become a fixed component of modern drug trade. In order to understand the mechanisms that make them successful and render law enforcement agencies (LEAs) relatively powerless, an analysis of the technologies employed and their interplay with the user behaviour and community culture of these darknet markets is in order. Simply pointing to cryptography is myopic and technologically deterministic, since it ignores the texture and specific environment it is embedded in. Instead, analysing socio-technical factors will yield more relevant results.

The paper begins by defining the core terms and definitions of darknet, deep web and dark web as used here, since the usage of these terms varies in the literature. Afterwards, darknet markets and their properties will be introduced through a literature review. Based on the various fields covered by the literature, the four fundamental market activities that darknet markets have to cover in order to operate successfully will be identified and analysed: 1. Transaction and communication, 2. Trust and reputation, 3. Payment and 4. Logistics, followed by a short discussion and conclusion.

Darknet, deep web or dark web?

Before diving into the analysis, the terminology of darknet markets needs some clarification, since there are multiple areas of research with slightly different research objects. The most ubiquitous, yet often misunderstood term is the darknet. Other terms are the deep web and the dark web.

By darknet, this paper refers to the encrypted overlay network of the internet, which is not publicly accessible (Mansfield-Devine, 2009). Instead, special clients like Tor have to be employed to facilitate a successful connection (Flick & Sandvik, 2013). However, this is a description of the type of connection and not the content found there.

On this technical overlay of the internet there exists an alternative to the openly accessible web, the so-called dark web. The dark web is often contrasted with the 'surface web', the part of the web that exists on the unencrypted internet (Bergman, 2001). Due to the nature of the darknet (which hosts the dark web), indexing individual pages and making them accessible to search engines is not possible (Rudesill, Caverlee & Sui, 2015). The entirety of all non-indexed pages in the internet is the so-called 'deep web' (Halevy & Madhaven, 2009). Besides the entire dark web, it also includes pages that cannot be indexed for other reasons. The content of social media pages is often only accessible from specific profile pages and intranets or otherwise protected content also belongs to the collection, making the deep web multitudes bigger than the dark web, and by some accounts even the entire visible internet (He et al, 2007).

Darknet-based research focuses on several phenomena. One of the earliest areas of darknet research focuses on peer-to-peer - or more specifically friend-to friend - file sharing networks like Napster or Pirate Bay with an emphasis on avoiding DRM (Wood, 2009; Acquisti, 2004). While file sharing is theoretically also possible in the dark web, the Tor infrastructure has low bandwidth and blocks traffic from file sharing (Tor FAQs, 2016), limiting it to the realm of P2P.

Another area of darknet research is focused on botnets, internet worms, and denial of services (DDoS) attacks, originating from unused address space, also called network telescopes or blackhole monitors (Bailey et al, 2006).

However, a current stream of research addresses phenomena on the dark web, focusing on areas ranging from religious and political extremism and terrorism in the darknet (Chen et al, 2008; L'huillier et al, 2010) through the specific technological infrastructure (Li et al, 2013) to a large amount of research on darknet markets, as detailed below.

This paper sets out to review the literature that concern these markets, with a focus on the socio-technical methods employed to guarantee their functionality.

Darknet markets

In a very similar fashion to Amazon, Ebay and other internet markets that digitised commerce to a great degree, darknet markets are digitising illegal black markets, for products ranging from false passports through stolen credit card information to small-scale firearms and other weapons. The biggest share of activity, however, is the digital drug market they created.

Like the entire dark web, darknet markets can only be accessed through means of encryption, like Tor or i2p. This reduces the possibility of tracing the location of vendors, buyers or marketplace operators and administrators to a great degree. A brief insight into the technical sight will follow later. All trades are settled in cryptocurrencies, with Bitcoin being the most popular one.

The size of dark markets is methodologically hard to measure, since market participants are anonymous, no taxes are paid and no accounting figures published. However, in the legal process against the founder of the first established darknet market Silk Road, the total turnover over the course of three years has been quantified as $1.2 billion (Barratt, Ferris & Winstock, 2014), while other researchers suggest a lower estimate of $22 million turnover per year (Phelps & Watt, 2014). At first sight, this seems almost negligible in the face of the annual global drugs trade that amounts to around $435 billion, as established by the United Nations Office on Drugs and Crime and Europol (UNODC, 2013).

However, for several reasons it is worth to investigate further. Most scholars agree that size and market share of illegal drug markets will keep increasing (Hardy & Norgaard, 2015), with some even projecting 'exponential growth' for hidden drug markets (Buxton & Bingham, 2015). The reasons for this are manifold. Efficiency gains of the darknet market have led to lower financial transaction costs (Brito & Castillo, 2013), improve transparency and quality of the drugs sold (Bancroft & Reid, 2015) and lower the prices through fierce competition (Martin, 2014), enabled by the global visibility of previously local drug distributors (Hardy & Norgaard, 2015).

Another difference is the type of users. It has been shown that the average user of darknet markets is younger and more likely to be male than the average drug user (Van Buskirk et al, 2016). In addition, the technical complexity and lack of violent aspects that often accompany and highly stigmatise street purchases of drugs lead to an appeal to a different target group of technically literate. On the side of the marketplace operators, advanced technical skills are necessary, and the motivations range from profit-orientation to idealist, often techno-libertarian convictions that all trades should be legal and possible (Bearman & Hanuka, 2015).

However, one of the central reasons for the sustained growth of darknet markets is the socio-technical infrastructure and culture of the darknet markets that renders identification of vendors and buyers very hard. The remainder of the paper analyses how darknet markets address various challenges posed by LEAs.

The core activities of dark markets

Unlike conventional online marketplaces, darknet markets offer almost entirely illegal products. This means, that in addition to the activities any online marketplace has to undertake, darknet markets need to operate under the scrutiny of LEAs.

This makes the entire operating procedure much harder, since each step has to be secure enough to withstand the scrutiny of LEAs. The purchase on darknet marketplaces can be broken down into four distinct activities. The current situation is a result of iterative learning of the entire community. New weaknesses were exposed after each market was taken down, since the evidence obtained had to be published in court. As a result, the current solutions are robust enough to allow functioning markets.

The activities cover the different phases and associated problems of each transaction and the resulting socio-technical solution.

- Activity 1: Transaction and communication

  How can seller and buyer interact anonymously without LEAs interfering?

- Activity 2: Trust and reputation

  How can the buyer trust the product arrives and is of adequate quality? How can the seller ensure the buyer pays?

- Activity 3: Payment

  How do darknet market participants avoid the money trail leading to their capture?

- Activity 4: Logistics: How can the products be delivered anonymously, even if either of the agents is a LEA?

Corresponding Author
Email Address: Bjoern.christian.wolf@gmail.com (B. C. Wolf)

1. Transaction and communication

An inherent difficulty of illegal drug markets is given by the very premise of the transaction. In order to obtain t he product, the buyer has to know the seller and communicate interest in a product. The seller communicates price and availability of the desired product. This precedes any possible transaction and this information facilitates the market. Without a knowledge of products and prices available, no transaction will happen.

Since the knowledge of the seller (or the facilitator of the trade, in cases of big platforms) is a requirement for most real world drug transactions, this has been a primary angle for LEAs, posing as interested parties and observing the typical transaction spots.

1.a Tor infrastructure

Darknet markets change this dynamic fundamentally. The first, and arguably most important aspect for Information Communication Technologies (ICT) is the underlying infrastructure, in particular the consistent use of the anonymisation software Tor – 'The Onion Router' (Flick & Sandvik, 2013).

Rather than directly arriving at the desired destination, each package and request is sent through a set of relay servers. Each server only knows the server it received the package from and the next server of the chain. None of the involved servers, however, knows the entire chain. This makes it impossible to connect a user with the website they requested. It is impossible for a server to infer the IP address, and thus location of a user.

On the website level, darknet pages have a top level domain ending in '.onion'. These links are only reachable via the eponymous Tor network. '.onion' is not recognised by the internet DNS root, the system to identify top-level domains like .com or .co.uk, but special browsers (like Tor browser or the specifically designed Tails system) can use it to operate through the dark web.

The second technical solution is PGP-encryption

"Pretty Good Privacy, or PGP, is a milestone in the history of cryptography, because for the first time it makes cryptography accessible to the wide mass of privacy hungry on-line public. PGP was created primarily for encrypting e-mail messages using public or conventional key cryptography. The latter are used mainly to encrypt local files. With public key cryptography, PGP first generates a random session key and encrypts the plaintext with this key. The session key along with the ciphertext are then encrypted using the recipient's public key and then forwarded to the recipient. Other features include generating message digests, generating digital signatures, management of personal 'key rings' and distributable public key certificates. It is also designed to work off-line to facilitate e-mail and file encryption, rather than on-line transactions" (Abdul-Rahman, 1997).

Following its intention as a 'cryptographic tool for the masses', PGP breaks the traditional hierarchical trust architecture and adopts the "web of trust" approach. There is no central authority which everybody trusts, but instead, individuals sign each other's keys and progressively build a web of individual public keys interconnected by links formed by this signatures (Abdul-Rahman, 1997).

2. Trust and reputation

With the technical anonymity, one crucial market activity has been addressed, and no party of a transaction can identify the other, nor can LEAs find out who participated in a transaction (and often even whether any transaction occurred). However, this complete anonymity leads to some adverse consequences. In offline sales, dealer and buyer know each other, which is the foundation of their trust. This is not the case online, since both parties are anonymous, trust comes less easy. Meanwhile, the illegal nature of the trade leads to trust being immensely important, both online and offline (Belackova & Vaccaro, 2013; Taylor & Potter, 2013).

In offline sales the exchange of money and product happens simultaneously, and any misunderstandings can be solved between the two parties involved. In the darknet markets, vendor and buyer have no obvious knowledge about their personalities, and no trivial mechanism to resolve conflicts (Hardy & Norgaard, 2015).

The product quality cannot be tested during the purchase process and the contract cannot be legally enforced, in case either of the parties involved does not deliver (Skarbek, 2008). In this realm of anonymity and lack of a central authority with the absence of government, new decentralised institutions are created to create trust and enable a functioning market (Leeson, 2010; Powell & Stringham, 2009).

2.a Trust - reputation mechanisms (rating and forums)

In order to deal with the uncertainties of vendor reliability, processing speed and product quality, many dark markets have implemented a rating mechanism, similar to e-commerce sites such as Amazon or Ebay.

The principle builds the very foundations of trust. It has been shown that repeated

play among individuals in a marketplace reduces moral hazard and other dishonest behaviour (Resnick and Zeckhauser, 2001). Darknet markets apply these mechanisms to repeated interactions between different individuals, but allow each individual to publish their satisfaction. Vendors both have average scores of the past months of operation, and it is also possible to read the specifics of single ratings, pointing out strengths and weaknesses in vendor reliability, processing speed and product quality.

In addition to the feedback on the vendor profiles, there are a range of forums dedicated to the trustworthiness of individual vendors, further increasing transparency

(Bancroft & Reid, 2015).

As a side effect of this transparent practice, vendors aim to proactively establish trust. In the offline world, many drug dealers only service known or recommended clients, while in online environments a proactive advertising of a product to previously unknown customers is possible (Tzanetakis et al, 2015).

The role of reputation in darknet markets can hardly be understated, or, as some have phrased it, "Reputation [...] is fundamental to the community's existence" (Hardy & Norgaard, 2015), since it is needed to create a functioning market in the absence of centralised power. In light of this decentralised coordination, some theorists have likened the dynamics of the darknet to the economic phenomenon of spontaneous order (Hardy & Norgaard, 2015; Leeson, 2010).

2.b Trust - Escrow:

The second mechanism employed to build trust is the escrow. Bitcoin payments are immediately valid and cannot be undone (unlike credit card payments that can be reversed), and likewise the product, once dispatched, cannot be returned to the sender, since "drug dealers do not provide return addresses" (Hardy & Norgaard, 2015). If the buyer receives the product first, he could simply refuse to pay. Likewise, if the vendor receives the money first, there is no guarantee the product will be dispatched. Therefore, a mechanism is needed to synchronise the transaction. Instead of sending the payment directly to the vendor, the buyer sends it to a neutral third party, either the marketplace operator, or, increasingly often, an outsourced, marketplace-independent escrow service (ibd).

Once the escrow provider confirms the receipt of the money, the vendor sends the product. After the buyer confirms delivery, the escrow provider pays the vendor. If a vendor never delivers, the escrow provider simply returns the money to the buyer, deducting only a small fee (Hu et al., 2004).

3. Payment - Bitcoin

Another point of failure for a successful drug market is payment processing. In offline drug deals, the preferred mode of payment is cash, since it cannot be traced easily. Online payments typically leave an electronic trail, deanonymising sender and recipient. Darknet markets employ pseudonymous cryptocurrencies like bitcoin for payment, a 'peer-to-peer, distributed payment system that offers its participants to engage in verifiable transactions without the need for a central third-party' (Christin, 2012).

In order to create a bitcoin wallet (can be thought of as a bank account for bitcoins), no documentation is needed. However, each wallet is entirely public, and the entire history of bitcoin movements of one wallet can be traced (Reid & Harrigan, 2012). This includes the initial conversion of an established currency like dollars into bitcoin. By following the origin of the money that was used to obtain drugs, LEAs can therefore theoretically identify the owner.

There are two ways to avoid this identification from happening. Services like local bitcoin or bitcoin ATMs allow the direct transfer of cash into bitcoin, therefore from an anonymous mode of payment into a pseudonymous one. However, this requires a real world interaction of the buyer, since he needs to handle the cash.

The other option are so-called bitcoin tumblers. Thousands of users each pay a few bitcoin into a tumbling service, the services mixes them and pays out an untraceable user. While it can be shown that a user was a part of a bitcoin tumbler, it is impossible to connect the bitcoins paid in to the bitcoins received (Van Hout, Bingham, 2013).

Tumblers are either operated by market places as a part of their offering or they can be used as standalone services for a small fee.

Through the interplay of pseudonymous bitcoin and the anonymisation mechanisms of cash payments and online tumblers, the money trail has been obfuscated and become very hard to trace.

4. Logistics

The final activity darknet markets have to address for a complete transaction is the distribution of the physical product. While the other three problems are mostly digital and can be resolved with encryption and electronic measures, the distribution necessarily happens in the physical world.

The most common way to distribute purchased goods are the traditional postal services. This way, the vendor faces an extremely low risk, since their address is not known and they simply dispatch a parcel in an anonymous mailbox (Tzanetakis et al, 2015).

In order for the buyer to obtain anonymity, several methods are used in practice. The delivery address can be a dead mailbox or a wrong name can be given for the correct address. This conceals the true identity of the buyer (Tzanetakis et al, 2015).

Other means undertaken are anonymous P.O. boxes and plausible deniability. Since darknet markets allow anyone to order drugs to any address, being the recipient of a drug shipment may not be sufficient proof.

In order to verify the buyer in cases of dead mailboxes or P.O. boxes, surveillance cameras or other surveillance measures are needed to capture the moment of pick-up. However, these operations are often costly, and the cost-benefit ratio is not positive. The buyers usually purchase small amounts of product, not enough for a commercial trafficking charge. In the offline world, these types of operation are often undertaken nevertheless, in order to create a link to the supplier. Since the design of darknet markets is in a way that the buyer has no specific knowledge about the supplier beyond forum posts

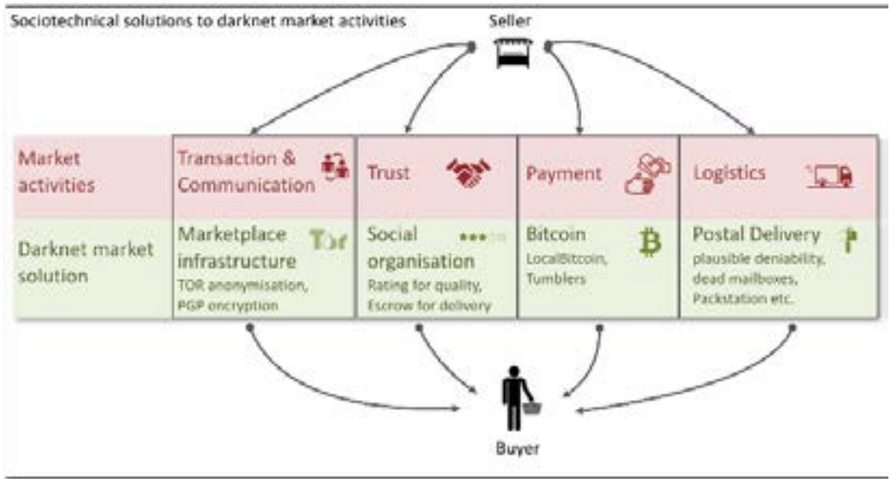

Figure 1: Socio-technical solutions to darknet market activities

and product feedback, this strategy makes no sense for online purchases (Martin, 2014).

Discussion

The review of the literature of darknet markets has brought to light an interesting situation. Darknet markets face a variety of unique challenges due to their illegal nature. ICTs like Tor and PGP allow communication and the transfer of information in anonymity. While this is a starting point for a functioning illegal online market it leads to two other issues. Firstly, anonymity is only as strong as its weakest link. Therefore, other parts of a transaction, like payments and delivery of the products, have to take place in anonymity as well. New technical solutions have emerged, like bitcoin as an electronic currency, anonymised via cash or bitcoin tumblers.

Logistics and distribution are made anonymous as well. The seller side has a very low risk by anonymously sending options of traditional postal services, while the buyers obfuscate their identity through methods like P.O. boxes under false names.

The combination of anonymity of communication and information, anonymous payments and anonymous shipping makes it very hard for LEAs to identify the transaction participants. Even occasional successes of LEAs against marketplaces do not result in widespread consequences, since market participants do not even know their counterparts' identity.

While this high degree of anonymity is an efficient protection against LEAs, it opens up problems of trust between vendors and buyers. This issue of trust is addressed in two ways. Vendors aim to establish a reputation through good ratings and reviews in the long run, while each individual transaction can be secured through a payment escrow service as well.

The mechanisms described require a degree of flexibility and willingness to acquire some technical expertise to operate in darknet markets. These higher transaction costs are partially set off by lower risks for market participants. Furthermore, research has shown that darknet markets 'reduce violence associated with illicit drugs', while also offering 'cheaper, higher quality products to drug consumers' (Martin, 2014). From a user perspective, they provide 'reliability, transparency, drug quality (mostly purity and potency)' (Bancroft & Reid, 2015) might help to further explain their emergence.

Conclusion

The study of darknet markets provides a unique insight into the emergence of alternative institutions in the absence of a legal framework and government power. Through repeated interactions and via trial and error, a proven set of social conventions and specific uses of technology emerged. The structure is much more decentralised than in traditional online marketplaces, yet the marketplace operators have the important task of facilitating interactions and providing a platform for vendors and buyers to operate.

Further research can be undertaken to understand how the iterative learning behaviour of market participants has led to the emergence of the concrete mechanisms we see today, as well as the concrete effect of the mechanisms employed by darknet markets on transaction costs.

References

Abdul-Rahman, A. (1997). The PGP Trust Model

Acquisti, A. (2004). Darknets, DRM, and trusted computing: Economic incentives for platform providers. In Workshop on Information Systems and Economics.

Bailey, M., Cooke, E., Jahanian, F., Myrick, A., & Sinha, S. (2006, March). Practical darknet measurement. In Information Sciences and Systems, 2006 40th Annual Conference on (pp. 1496-1501). IEEE.

Bancroft, A., & Reid, P. S. (2015). Concepts of illicit drug quality among darknet market users: Purity, embodied experience, craft and chemical knowledge. International Journal of Drug Policy.

Barratt, M. J., Ferris, J. A., & Winstock, A. R. (2014). Use of Silk Road, the online drug marketplace, in the United Kingdom, Australia and the United States. Addiction, 109(5), 774-783.

Bearman, J., & Hanuka, T. (2015). The Rise and Fall of Silk Road, (Part 1): Ross Ulbricht's journey from libertarian idealist to savage kingpin. Wired, 23(5), 90-97.

Belackova, V., & Vaccaro, C. A. (2013). "A Friend With Weed Is a Friend Indeed": Understanding the Relationship Between Friendship Identity and Market Relations Among Marijuana Users. Journal of drug issues, 0022042613475589.

Bergman, M. K. (2001). White paper: the deep web: surfacing hidden value. Journal of electronic publishing, 7(1).

Biddle, P., England, P., Peinado, M., & Willman, B. (2002, November). The darknet and the future of content distribution. In ACM Workshop on Digital Rights Management (Vol. 6, p. 54).

Brito, J., & Castillo, A. (2013). Bitcoin: A primer for policymakers. Mercatus Center at George Mason University.

Buxton, J., & Bingham, T. (2015). The Rise and Challenge of Dark Net Drug Markets. Policy Brief 7, Global Drug Policy Observatory.

Chen, H., Chung, W., Qin, J., Reid, E., Sageman, M., & Weimann, G. (2008). Uncovering the dark Web: A case study of Jihad on the Web. Journal of the American Society for Information Science and Technology, 59(8), 1347-1359.

Christin, N. (2013, May). Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. In Proceedings of the 22nd international conference on World Wide Web (pp. 213-224). International World Wide Web Conferences Steering Committee.

Flick, C., & Sandvik, R. A. (2013). Tor and the darknet: researching the world of hidden services. The possibilities of ethical ICT, 150.

Halevy, A., & Madhaven, J. (2009). What Is the Deep Web?, published in Segaran, T., & Hammerbacher, J. (2009). Beautiful data: the stories behind elegant data solutions. " O'Reilly Media, Inc.".

Hardy, R. A., & Norgaard, J. R. (2015). Reputation in the Internet black market: an empirical and theoretical analysis of the Deep Web. Journal of Institutional Economics, 1-25.

He, B., Patel, M., Zhang, Z., & Chang, K. C. C. (2007). Accessing the deep web. Communications of the ACM, 50(5), 94-101.

Leeson, P. T. (2010). Anarchy Unbound: How Much Order Can Spontaneous Order Create?, Cheltenham, UK and Northampton, MA: Elgar.

L'huillier, G., Ríos, S. A., Alvarez, H., & Aguilera, F. (2010, July). Topic-based social network analysis for virtual communities of interests in the dark web. In ACM SIGKDD Workshop on Intelligence and Security Informatics (p. 9). ACM.

Li, Z., Alrwais, S., Xie, Y., Yu, F., & Wang, X. (2013, May). Finding the linchpins of the dark web: a study on topologically dedicated hosts on malicious web infrastructures. In Security and Privacy (SP), 2013 IEEE Symposium on (pp. 112-126). IEEE.

Mansfield-Devine, Steve (December 2009). "Darknets". Computer Fraud & Security. 2009 (12): 4–6.

Markopoulos, P., Xefteris, D., & Dellarocas, C. (2015). Manipulating Reviews in Dark Net Markets to Reduce Crime.

Martin, J. (2014). Lost on the Silk Road: Online drug distribution and the 'cryptomarket'. Criminology and Criminal Justice, 14(3), 351-367.

Phelps, A., & Watt, A. (2014). I shop online–recreationally! Internet anonymity and Silk Road enabling drug use in Australia. Digital Investigation,11(4), 261-272.

Powell, B., & Stringham, E. P. (2009). Public Choice and the Economic Analysis of Anarchy: A Survey. Public Choice, 140(3/4), 503–538.

Reid, F., & Harrigan, M. (2012). An Analysis of Anonymity in the Bitcoin System. In Security and Privacy in Social Networks (pp. 197-223).

Resnick, P., & Zeckhauser, R. (2002). Trust among strangers in internet transactions: Empirical analysis of ebay's reputation system. The Economics of the Internet and E-commerce, 11(2), 23-25.

Rudesill, D. S., Caverlee, J., & Sui, D. (2015). The Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box. Woodrow Wilson International Center for Scholars, STIP, 3.

Skarbek, E. S. (2008), Remittances and Reputations in Hawala Money-Transfer Systems: Self-Enforcing Exchange on an International Scale. Journal of Private Enterprise, 24(1), 95–117.

Steward, K. (2013). THE 21 st CENTURY'S SILK ROAD.

Taylor, M., & Potter, G. R. (2013). From" Social Supply" to" Real Dealing": Drift, Friendship, and Trust in Drug Dealing Careers. Journal of Drug Issues, 0022042612474974.

Tor project FAQs (retrieved 2016): https://www.torproject.org/docs/faq.html.en

Tzanetakis, M., Kamphausen, G., Werse, B., & von Laufenberg, R. (2015). The transparency paradox. Building trust, resolving disputes and optimising logistics on conventional and online drugs markets. International Journal of Drug Policy.

UNODC. (2013). World Drug Report 2013.

Van Buskirk, J., Roxburgh, A., Bruno, R., Naicker, S., Lenton, S., Sutherland, R., ... & Burns, L. (2016). Characterising Dark Net Marketplace Purchasers in a Sample of Regular Psychostimulant Users. International Journal of Drug Policy.

Van Hout, M. C., & Bingham, T. (2013). 'Silk Road', the virtual drug marketplace: A single case study of user experiences. International Journal of Drug Policy, 24(5), 385-391.

Von Lohmann, F. (2004). Measuring the Digital Millennium against the Darknet: Implications for the regulation of technological protection measures. Loy. LA Ent. L. Rev., 24, 635.

Wehinger, F. (2011, September). The Dark Net: Self-Regulation Dynamics of Illegal Online Markets for Identities and Related Services. In Intelligence and Security Informatics Conference (EISIC), 2011 European (pp. 209-213). IEEE.

Wood, J. A. (2009). Darknet: A Digital Copyright Revolution, The. Rich. JL & Tech., 16, 1.