Meropi Tzanetakis

18 Darknet

Abstract: This chapter explores the dual nature of the darknet, providing insights for students and criminologists alike. It examines how the darknet serves as a digital environment for both protecting privacy and freedom of expression and facilitating criminal activities, all rooted in a shared desire to evade commercial and state surveillance. By analyzing the enabling and constraining elements of the Janus-faced darknet, the chapter illustrates these dynamics through a detailed discussion of darknet drug distribution platforms, drawing on the author's original research.

Keywords: platforms, user data, encryption, privacy, surveillance, illicit drugs

The term darknet or dark web initially suggests something mystical, criminal, and threatening. In fact, however, darknet is not referring to the legal status of the content, but rather how certain services can be accessed on the internet (Tzanetakis, 2018). By crawling and analyzing darknet pages, Avarikioti et al. (2018) found that approximately 60 % of the content is legal, with illegal services including fraud, counterfeit offers, and drug markets. More broadly, darknet can be distinguished from the surface web or clearnet, which is accessible by search engines, and the deep web, which requires the user to take additional steps such as logging in or making a payment to access the content.

The internet can be imagined as an iceberg in the ocean with its visible tip being the surface web but only accounting for roughly about 10 % of the content. The much larger part of the iceberg is below the ocean and is referred to as the deep web with its content being invisible as it is inaccessible for search engines. The deep web comprises intranets of companies or organizations, as well as user accounts, among other elements. The darknet is then a small subset of the deep web that contains hidden services that are only accessible with specialized software.

To get access to the hidden services, encryption software like the TOR Browser (The Onion Router), Freenet, I2P (Invisible Internet Project) is required. In regular internet traffic, data moves between a user and its destination directly, often leaving identifiable traces. The darknet, however, facilitates network anonymity by routing the internet traffic through a series of randomly chosen servers. This process conceals the user's IP address and location, complicating law enforcement interventions. Technically, the darknet consists of a variety of darknets. In the following, the term darknet is used collectively for all darknets. By making use of TOR, users can communicate almost anonymously, ensuring no data is disclosed that could reveal their identity or whereabouts. However, the term darknet is misleading, as it implies that all content may be legally restricted, which is not necessarily the case as it contains a variety of content from file sharing to pornographic material, and from leaked data to drug markets.

https://doi.org/10.1515/9783111062037-019

From privacy and freedom to surveillance and control

The darknet presents a Janus-faced digital environment, intriguing beyond its inherent mystery. It encompasses both privacy and freedom while entangled with elements of control and surveillance. On one side, it offers heightened privacy and anonymity, fostering uncensored communication and information exchange. Its encryption offers shelter for activists, journalists, and dissidents seeking to evade censorship, surveillance, and oppressive regimes. Conversely, it functions as a platform facilitating illicit activities, enabling illicit trade and criminal exchanges under the veil of anonymity. Initially, this duality presents a paradox: while providing refuge for the marginalized, it also facilitates persons engaged in criminal activities, encapsulating the complexity of the darknet. This supposed duality makes the darknet a compelling and intricate subject for criminological exploration. In this chapter, I will disentangle the darknet by arguing that both privacy and freedom of expression—regardless of whether it involves supporting fundamental human rights or criminal activities—have the same origin: they aim to circumvent and resist commercial or state control and surveillance. I will illustrate the Janus-faced darknet with my own research on darknet drug distributing platforms (Tzanetakis and South, 2023).

When browsing through the surface web or deep web, internet users leave digital traces, encompassing identifiable elements like IP addresses, cookies, and cache data, vital for website personalisation (Tzanetakis and Marx, 2023). Additionally, browser history, search queries, and login information contribute to a digital footprint. These traces form a digital trail, enabling websites to personalize content and facilitate tailored user experiences. However, they also raise significant privacy concerns as the traces can be utilized for targeted advertising, potentially invasive tracking, or even surveillance, emphasizing the impact of online activities on user privacy. They underscore the intricate balance between personalization and the potential exploitation of user data for commercial or monitoring purposes.

User-generated content is subject to monitoring, collection, and analysis by various actors, including the digital information economy. The design of digital platforms encourages their users to engage in prosumption practices which means that individuals function as both producers and consumers of content within a platform (Srnicek, 2017). These practices include activities such as uploading and sharing of content with others and using a ‘like’ button, tweet, or hashtag while swiping through text, video, audio, and pictures produced by other prosumers. Digital platforms engage in prosumption practices with the aim of monetizing the production and consumption of information, seeking to derive financial value from the digital data generated by users (Zuboff, 2019). With the advent of new practices and technologies, surveillance has become widespread and pervasive.

In contrast to commercial surveillance which focuses on collecting consumer data for marketing, profit, or service personalization, state-driven surveillance is primarily conducted by government or law enforcement agencies, aiming to monitor and control citizens for reasons such as national security, law enforcement, and social control (Bauman and Lyon, 2013). The extent of surveillance on a global scale was uncovered by the Snowden files which revealed, among other things, mass data collection from private phone records and internet activities of both citizens and leaders worldwide (Lyon, 2014). The revelations demonstrated a critical breach of individual privacy and civil liberties, showing how citizens, irrespective of suspicion, were subjected to mass surveillance. This undermined the fundamental principles of democracy, fostering an environment of suspicion and eroding trust between governments and the general public. The broad and non-targeted data collection raised ethical concerns, highlighting the potential for abuse and the imbalance between security measures and personal freedoms.

The convergence of state-driven and commercial digital surveillance, aimed at behavioral regulation, control imposition, and profit generation, serves as a fertile environment for the emergence of the darknet. Within this digital realm, the darknet thrives by offering heightened privacy, freedom of expression, and access to information, enabling users to navigate digital spaces and communicate via digital media with increased anonymity. This, however, supports both fundamental human rights and criminal activities by enabling individuals to avoid censorship and disguising users' digital traces. Both share a common genesis by aiming to bypass and oppose control and surveillance by commercial industry or governmental bodies. Fundamental human rights and criminal activities initially appear to be diametrically opposed. In the following, I will use the example of my own original research on darknet drug platforms to disentangle this paradox.

Researching darknet drug platforms

Darknet drug platforms or cryptomarkets are technological infrastructures mediating exchange of a wide range of illicit drugs, among other products and services, between vendors and consumers (Tzanetakis and Marx, 2023). These digital platforms have been described as a "transformative criminal innovation" (Aldridge and Décary-Hétu, 2014) combining anonymizing technologies (e. g., TOR browser) with cryptocurrencies (e. g., Bitcoin) as a decentralized and non-government-issued means of payment (Barratt and Aldridge, 2016). In combination, these technologies enable its users to separate their identity from their cryptomarket activity, e. g., browsing through the offers, creating an account, or ordering illicit drugs.

The affordances of the darknet have contributed to a "transparency paradox" (Tzanetakis et al., 2016). While the platform operator organizes the marketplace, hosts multiple sellers, and defines the basic terms and conditions, sellers and buyers remain anonymous or pseudonymous while publicly organizing market exchanges. Acknowledged as unprecedented, the quality and availability of this data have introduced novel sets of data available to researchers (Barratt and Aldridge, 2016).

The darknet is a dynamic and ever-evolving environment on the internet (Tzanetakis and South, 2023). Characterized by frequently changing websites and a fluid landscape, it operates with an inherent volatility. While the content on the darknet spans the whole continuum of legality and illegality, particularly when associated with clandestine activities, websites in this realm are often short-lived and may involve sophisticated scams. The swift adaptations and constant shifts in online spaces pose challenges for research (as well as law enforcement), requiring a flexible approach to navigate the rapidly changing environments of illicit online activities (see Researching Online Forums by Šupa). Drug markets per se are also a fragmented and fluid research field, which changes over time and in reflection of societal developments, in order to avoid attention of the police.

Digital ethnography involves immersing oneself in online environments, to understand social phenomena from the participants' perspectives (Hine, 2015; Tzanetakis, 2021). While the method of digital ethnography is flexible and adaptable, it underscores the importance of contextualizing data in our globalized, translocal, and digitally interconnected world, considering both local meanings and the impacts of internet commercialization (see Online Ethnography by Gibbs and Hall).

The process involves an initial phase of inhabiting the digital environment to explore the hard-to-reach communities of darknet drug platform users (Tzanetakis, 2019). These communities consist of platform operators, customers, dealing customers, small-level dealers, high-level dealers, moderators, information hubs, law enforcement, researchers, journalists, and interested people who are browsing through platforms and discussion forums. For my research, this meant engaging in participant observation, including the user-generated content by self-presentations of vendors as well as monitoring of interactions between customers, operators, moderators, and vendors on various cryptomarkets and associated discussion forums. I also took screenshots and wrote field notes about my observations and perceptions. For the researcher, immersion serves the purpose of learning how to understand local meanings and familiarizing themselves with the specific cultural behaviors and norms.

The next digital ethnographic phase involves getting meaningful access to the hard-to-reach online community (Kaufmann and Tzanetakis, 2020). Field entry is influenced by following the cultural norms and rituals of the specific online community (see Accessing Online Communities by Kaufmann). For marginalized people to open up, a researcher needs to position themself as a cultural insider or outsider or both at the same time. Attaining cultural insider status necessitates the researcher sharing commonalities, roles, or experiences that resonate with the community under exploration. Adler and Adler (1987) identified three membership roles for qualitative researchers: peripheral, active, and complete. While Barratt and Maddox (2016) performed an active membership role in the darknet drug community with Barratt volunteering as administrator of a drug harm-reduction forum that was respected within the community, I adopted a peripheral membership role enabling me to simultaneously inhabit the roles of an insider and an outsider. A critical consideration for researchers lies in the choice between adopting a pseudonym, often advantageous for obtaining institutional ethical approval, and entering the field openly, potentially promoting access and trust. However, opting for a pseudonym raises ethical dilemmas regarding transparency and authenticity within the research process. Balancing these factors is essential for maintaining research integrity and navigating the complexities of building relationships within the community studied.

My lack of complete immersion in the social world studied resulted in my being perceived as a cultural outsider. Simultaneously, I positioned myself as a cultural insider by acquiring the technological knowledge standards prevalent in the hard-to-reach darknet community. As I gained knowledge about the digital technologies employed, the operational dynamics of the ecosystem of darknet platforms, insights into vulnerabilities concerning law enforcement and fraud, as well as familiarity with the specific language and abbreviations, I consistently upheld a transparent researcher position. Moreover, forum moderators played an important role as gatekeepers to reassure the hard-to-reach online communities that my research was legitimate. Attaining complete membership within the darknet drug market community raises ethical concerns in research and may, in certain instances, cast doubt on the scientific validity of the research results. This role may involve the researcher actively engaging in unlawful activities. However, it provides the most comprehensive access to the community under study.

As part of this digital ethnographic phase, I was able to establish a credible online presence with the research participants in order to gain meaningful access to the darknet drugs community (Kaufmann and Tzanetakis, 2020). For my research, data collection included qualitative interviews with members of the hard-to-reach darknet drug market community, screenshots of interactions between community members on drug platforms and related discussion forums, screenshots of vendor shops, customer ratings, and field notes on observations of social practices.

Ethical considerations

Empirical research on darknet drug platforms comes with a variety of ethical considerations and challenges such as if the data available can be considered public or private, gaining participant's informed consent, ensuring anonymity, and protecting both researchers and research participants. And although this chapter cannot cover all ethical implications related to cryptomarket research, other chapters in this handbook as well Martin and Christin (2016) and Lavorgna and Holt (2021) are well positioned to further explore the multifaceted ethical challenges. Nevertheless, I would like to briefly address some key research ethical dimensions here. The affordances of the darknet present distinct challenges that deviate slightly from conventional ethical standards.

My research on darknet drug market practices includes sensitive research questions about activities that are considered criminal offenses in most jurisdictions. Accordingly, de-anonymizing participants can have legal consequences, even if this happens accidently. At the same time, establishing trust with community members is essential when conducting digital ethnography. Here, the knowledge I gained about encryption software and specific settings that prevent detection by law enforcement are pertinent. Using suitable 'operational security' measures including non-traceable software (Jabber/XMPP messaging service with Off-the-Record messaging encryption) helped me to establish credibility in the field. In my interviews, I made sure not to collect identifying information (e. g., names, locations) and anonymize the data as soon as possible afterwards. This demonstrates that ethical considerations require navigating a delicate balancing to ensure the protection of research participants.

Thus, researchers first need to develop a sufficiently nuanced understanding of the specific digital environment, adhere to legal and regulatory policies including ethical guidelines of professional organizations such as the Association of Internet Researchers (AoIR) (franzke et al., 2020). Secondly, ethical decisions should be context-dependent, meaning they vary depending on the social and cultural context in which information is shared and exchanges occur (Nissenbaum, 2009). Thirdly, Markham (2018) introduced an impact model of ethics which emphasizes the potential consequences and effects of one's research. It involves evaluating how anything we do in the name of research is directly relevant to the community studied. Rather than merely harvesting digital interactions for our research aims, the focus should be on designing studies that enact social change within communities. This approach extends to considering how research influences the shape of possible futures, highlighting a holistic and socially responsible perspective on the impact of our research endeavours.

Disentangling the paradox of the darknet

At the first sight, darknet drug markets could be perceived as a threat due to their role in facilitating the anonymous buying and selling of illicit drugs, challenges in law enforcement efforts, and challenges for traditional drug control strategies. However, a more holistic perspective suggests that the growth of cryptomarkets is associated with a potential to reduce a variety of drug related harms (Aldridge et al., 2018; Bancroft, 2017; Barratt et al., 2016; Tzanetakis and von Laufenberg, 2016). Harm reduction is a public health approach that aims to minimize negative consequences, such as overdose and disease transmission, without necessarily advocating for abstinence (Lenton and Single, 1998). It includes strategies like needle exchange programs, supervised consumption rooms, and education to promote safer practices.

Darknet drug markets facilitate harm reduction by offering transparency on drug quality and purity of the drugs compared to traditional distribution channels. This factor holds significance because certain harms are linked to the potential for adulteration and the broader composition of drugs, leading to undesired effects or the risk of overdose. Another harm reduction benefit is minimizing physical and psychological violence for users compared to traditional transactions. Facilitated through features like the escrow payment system, the platform operator manages funds between transaction parties, preventing fraud and fostering trust. The operator serving as an intermediary, this practice ensures financial oversight until the drugs are delivered as agreed upon. A third harm reduction aspect revolves around peer-to-peer information exchange on discussion forums and via rating systems to promote safer practices. They are used among peers to share experiences and information about the qualities of the drugs, effects, dosage recommendations, and polydrug use. Yet, these harm reduction aspects also involve surveillance activities entangled with encrypted data traffic. While harm reduction efforts aim to enhance safety, the encrypted data traffic also allows for the tracking and analysis of user interactions, transactions, and information exchange. This surveillance could potentially be carried out by various actors, including law enforcement agencies or other private actors interested in monitoring activities on these platforms.

A nuanced understanding of cryptomarkets reconciles the perceived contradiction of the darknet—a space for both criminal activities and marginalized free expression. Distributing drugs on darknet platforms is criminal, yet this environment minimizes harm from punitive measures. Amid the dual nature of the darknet, the emergence of new criminal offenses and expanding surveillance warrant careful consideration, balancing privacy, civil liberties, and the complex dynamics of this Janus-faced digital realm.

Suggested reading

Gehl, R. (2018). *Weaving the Dark Web: Legitimacy on Freenet, Tor, and I2P.* Cambridge, MA: MIT Press.

Lavorgna, A. (2020). *Cybercrimes: Critical Issues in a Global Context.* London: Macmillan.

Martin, J., Cunliffe, J., & Munksgaard, R. (2019). *Cryptomarkets. A Research Compendium.* Bingley: Emerald

Mirea, M., Wang, V., & Jung, J. (2019). The not so dark side of the darknet: A qualitative study. *Security Journal*, 32, 102 – 118.

References

Adler, P., & Adler, P. (1987). *Membership Roles in Field Research.* Newbury Park, CA: Sage.

Aldridge, J., & Décary-Hétu, D. (2014). Not an ‘Ebay for drugs’: The cryptomarket ‘Silk Road’ as a paradigm shifting criminal innovation. DOI: 10.2139/ssrn.2436643

Aldridge, J., Stevens, A., & Barratt, M. J. (2018). Will growth in cryptomarket drug buying increase the harms of illicit drugs? *Addiction*, 113(5), 789 – 796.

Avarikioti, G., Brunner, R., Kiayias, A., Wattenhofer, R., & Zindros, D. (2018). Structure and content of the visible Darknet. arXiv preprint arXiv:1811.01348.

Barratt, M. J., & Aldridge, J. (2016). Everything you always wanted to know about drug cryptomarkets* (*but were afraid to ask). *International Journal of Drug Policy*, 35, 1 – 6.

Bancroft, A. (2017). Responsible use to responsible harm: Illicit drug use and peer harm reduction in a darknet cryptomarket. *Health, Risk & Society*, 19(7 – 8), 336 – 350.

Barratt, M. J., & Maddox, A. (2016). Active engagement with stigmatised communities through digital ethnography. *Qualitative Research*, 16(6), 701 – 719.

Barratt, M. J., Ferris, J., & Winstock, A. R. (2016). Safer scoring? Cryptomarkets, social supply and drug market violence. *International Journal of Drug Policy*, 35, 24 – 31.

Bauman, Z., & Lyon, D. (2013). *Liquid Surveillance: A Conversation.* Cambridge: Polity Press.

franzke, a.s., Bechmann, A., Zimmer, M., Ess, C., & the Association of Internet Researchers (2020). *Internet Research: Ethical Guidelines 3.0.* https://aoir.org/reports/ethics3.pdf.

Hine, C. (2015). *Ethnography for the Internet: Embedded, Embodied and Everyday.* London: Bloomsbury.

Kaufmann, M., & Tzanetakis, M. (2020). Doing internet research with hard-to-reach communities: Methodological reflections on gaining meaningful access. *Qualitative Research*, 20(6), 927 – 944.

Lavorgna, A., & Holt, T. J. (eds.) (2021) *Researching Cybercrimes: Methodologies, Ethics and Critical Approaches.* Cham: Palgrave Macmillan.

Lenton, S., & Single, E. (1998). The definition of harm reduction. *Drug and Alcohol Review*, 17(2), 213 – 220.

Lyon, D. (2014). Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big Data & Society*, 1(2), 1 – 12.

Markham, A. N. (2018). Afterword: Ethics as Impact—Moving from error-avoidance and concept-driven models to a future-oriented approach. *Social Media + Society*, 4(3).

Martin, J., & Christin, N. (2016). Ethics in cryptomarket research. *International Journal of Drug Policy*, 35, 84 – 91.

Mayorga-Gallo, S., & Hordge-Freeman, E. (2017). Between marginality and privilege: Gaining access and navigating the field in multiethnic settings. *Qualitative Research*, 17(4), 377 – 394.

Nissenbaum, H. (2009). *Privacy in Context: Technology, Policy, and the Integrity of Social Life.* Stanford: Stanford University Press.

Srnicek, N. (2017). *Platform Capitalism.* Cambridge: Polity Press.

Tzanetakis, M. (2018). The darknet's anonymity dilemma. In A. von Humboldt Institute for Internet and Society (ed.), *Encore 2017. The Annual Magazine on Internet and Society Research* (pp. 118 – 125). Berlin: HIIG.

Tzanetakis, M. (2019). Informal governance on cryptomarkets for illicit drugs. In A. Polese, A. Russo, & F. Strazzari (eds.), *Governance Beyond the Law: The Immoral, The Illegal, The Criminal* (pp. 343 – 361). Basingstoke: Palgrave Macmillan.

Tzanetakis, M. (2021) Qualitative Online-Forschungsmethoden: Digitale Datenerhebung und ethische Herausforderungen. In B. Prainsack & M. Pot, *Qualitative und interpretative Methoden in der Politikwissenschaft* (pp. 130 – 141). Wien: Facultas.

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.

Tzanetakis, M., & Marx, S. (2023). The dark side of cryptomarkets: Towards a new dialectic of self-exploitation within platform capitalism. In M. Tzanetakis & N. South (eds.), *Digital Transformations of Illicit Drug Markets: Reconfiguration and Continuity* (pp. 141 – 154). Bingley: Emerald.

Tzanetakis, M., & South, N. (eds.) (2023). *Digital Transformations of Illicit Drug Markets: Reconfiguration and Continuity.* Bingley: Emerald.

Tzanetakis, M., & von Laufenberg, R. (2016). Harm Reduction durch anonyme Drogenmärkte und Diskussionsforen im Internet? In akzept e.V. Bundesverband für akzeptierende Drogenarbeit und humane Drogenpolitik: 3. Alternativer Drogen- und Suchtbericht 2016 (pp. 189 – 194). Lengerich: Pabst Science.

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* London: Profile Books.