Article

Journal of Contemporary Criminal Justice
2023, Vol. 39(2) 276–297

DOI: 10.1177/10439862231159530
journals.sagepub.com/home/ccj
SAGE

Keeping Pace With the Evolution of Illicit Darknet Fentanyl Markets: Using a Mixed Methods Approach to Identify Trust Signals and Develop a Vendor Trustworthiness Index

Marie-Helen Maras[1], Jana Arsovska[1], Adam Scott Wandt[1], and Kenji Logie[1]

Abstract

Illicit darknet markets (DNMs) are highly uncertain and in a perpetual state of flux. These markets thrive in a zero-trust, high-risk environment. However, the trustworthiness of vendors plays a critical role in illicit transactions and the sustainability of the illegal trade of goods and services on DNMs. Focusing on the illicit fentanyl trade and applying signaling theory and embedded mixed methods design, we examined different ways that trustworthiness is signaled by vendors on darknet sites. Fentanyl, a synthetic opioid, in recent years, has been declared a public health emergency in the United States due to its high potency and unprecedented number of deaths associated with its use; however, the topic remains understudied and requires urgent attention. There are few studies that have focused on fentanyl trafficking on DNMs and no mixed method studies that have focused specifically on trust signals in DNM fentanyl networks. In our research, first, we conducted a focus group and in-depth interviews with criminal justice professionals to understand the inner workings of darknet sites, fentanyl networks, and how trust is assessed. Second, we scraped select darknet sites to collect and curate scraped data for later examination of vendor trustworthiness on DNMs. Third, using signaling theory to

[1]City University of New York, USA

Corresponding Author:
Marie-Helen Maras, Associate Professor, Department of Security, Fire, and Emergency Management, John Jay College of Criminal Justice, City University of New York, 524 W 59 St., New York, NY 10019, USA.
Email: mmaras@jjay.cuny.edu

understand how vendors signal trustworthiness on select darknet sites selling drugs, including fentanyl, we applied both qualitative and quantitative content analysis of DNM features, and language used in vendor profiles, listings, and product/vendor reviews, to inform the development of a trustworthiness index. In this research, we used software, such as Atlas.ti and Python, to analyze our data. The main purpose of this article is to provide an in-depth description of the mixed methods approach we used to inform the development of a vendor trustworthiness index, which we used to examine trust between illicit fentanyl vendors and buyers. Our research can serve as a guide for the development of DNM vendor trustworthiness index for future research on other illegal markets.

Keywords
signaling theory, trust, darknet, fentanyl, mixed methods, embedded research design

Introduction

Synthetic opioids, particularly fentanyl, are a leading cause of opioid deaths in the United States. According to the Centers for Disease Control and Prevention (CDC, 2022), U.S. overdoses from opioids rose from 70,029 in 2020 (57,834 of these deaths were linked to synthetic opioids) to 80,816 in 2021 (of which 71,238 were attributed to synthetic opioids). The U.S. Drug Enforcement Administration (DEA, 2021) identified "illicit fentanyl" as "primarily responsible for fueling the ongoing opioid crisis" (p. 4). Synthetic opioids, like fentanyl and tramadol, are also cheaper to manufacture and buy than other opioids (Miller, 2020). The costs of fentanyl and its high potency are viewed as drivers for its increased use by traffickers, dealers, and even buyers. The DEA further identified that drug traffickers and dealers mix illegal fentanyl with other illicit drugs, like heroin and other illegal drugs. Buyers may wittingly or unwittingly purchase fentanyl and/or other illicit drugs (opioids and non-opioid drugs) mixed with fentanyl.

A factor that contributed to the mass distribution and illegal purchasing of synthetic opioids, including fentanyl, was the availability of these illicit drugs on darknet marketplaces (DNMs; Miller, 2020). In violation of the U.S. Controlled Substances Act of 1970, drugs, including fentanyl, have been traded in DNMs, which have removed barriers to entry into illicit drugs markets by providing criminals with the infrastructure, personnel, resources, clientele, and products needed to sell drugs online (Maras, 2017). These illegal drugs have been advertised, marketed, and sold via smartphone apps and on bulletin boards, discussion forums, social media platforms, online marketplaces, online classified advertisement sites, instant messaging platforms, and unencrypted, encrypted, and proprietary communications platforms (e.g., Facebook Messenger, WhatsApp, and PhantomSecure; see UNODC, 2021). Drug markets in general, and those on the darknet specifically, are in a constant state of flux (UNODC, 2021, 2022), where the type and variation of drugs, demand and supply for certain drugs, market

structures and networks, interactions within networks, and major players within markets, among other things, frequently change.

DNMs are resilient and thrive in a zero-trust, high-risk environment. The trustworthiness (i.e., a trait of being honest and reliable) of vendors plays a critical role in illicit transactions and the sustainability of the illegal trade of goods and services, such as drugs, on DNMs. However, there is limited research on trustworthiness and DNMs, including the variety of signals used to communicate vendor trustworthiness. By drawing on literature in criminology, economics, and business, and by using the illicit fentanyl trade as an example, the main objective of this study is to provide a detailed description of the ways in which an embedded mixed methods approach can be used to inform the development of a vendor trustworthiness index. Vendors communicate their trustworthiness through signals on their profiles, listings, and comments in discussion forums, among other things; thus, this article illustrates the methods researchers can use to collect and analyze data needed for the development of a DNM vendor trustworthiness index.

Literature Review

Signaling theory focuses on the deliberate signals used to communicate positive attributes or negative attributes when information symmetry is present (Fischer & Reuber, 2007). This theory further provides insights into why certain signals are reliable or unreliable (Connelly et al., 2011). Signaling theory has been used to study interactions and behaviors in the fields of economics, management, entrepreneurship, marketing, human resource management, biology, anthropology, and criminology (e.g., Bird & Smith, 2005; Connelly et al., 2011; Gambetta, 2009; Kirmani & Rao, 2000; Maynard-Smith & Harper, 1995; Riley, 2001; Spence, 1973, 2002). This theory has also been applied to the study of legal markets and illegal markets (e.g., Connelly et al., 2011; Gambetta, 2009).

Furthermore, signaling theory has been used as a lens to examine the illicit goods and services trade on clearnet markets, forums, and social media platforms (e.g., Facebook), including illegal carding forums and drug markets (e.g., Décary-Hétu & Leppänen, 2016; Holt et al., 2016; and Bakken, 2021). Décary-Hétu and Leppänen (2016), in their study of online carding forums, identified social ties as positively correlated to criminal opportunities (i.e., criminals' success on these forums) and the lifespan of criminal actors on criminal markets (i.e., period of time a criminal is part of and/or engaged with criminal markets), which is viewed as a sign of criminal reliability, as hard to mimic signs of criminal performance. Similarly, Holt et al. (2016), had, among other factors, identified the lifespan of criminal actors on online carding forums (i.e., *user status*), particularly in the form of "long-term participation on the market," as an indicator of trust (p. 144). Prior research also identified the length of time vendors are active on the sites (e.g., number of posts and other activity) and the status of the vendor on the criminal sites (i.e., their rank) as signals of trust (Décary-Hétu & Laferrière, 2015). More recently, Bakken (2021) examined Facebook profiles of drug dealers to identify signals of trust. He found that cultural indicators (i.e.,

cultural codes to sell drugs, such as emojis and code words) were viewed as signals of trustworthiness. He further found "professional" Facebook profiles, which clearly expressed the sale of illicit drugs, even including pictures of them, contained the following trust signals: customer service ("express delivery"), words describing quality of drugs (e.g., "high quality"), brands, and were up and running for a significant period of time. Overall, Bakken's (2021) study emphasized the importance of understanding that there are trust indicators beyond those linked to vendor reputation and assessed through buyer feedback.

Unlike clearnet markets, there are few studies that have applied this theory to study DNM interactions (e.g., Hardy & Norgaard, 2016; Laferrière & Décary-Hétu, 2023). Hardy and Norgaard (2016) analyzed the Silk Road DNM to identify different measures of a vendor's reputation based on vendor and product rating, finding that most vendor reputation information is found in product ratings. The authors conclude that building a good reputation on DNMs enables vendors to charge premium prices for the goods and services they offer, thereby further incentivizing vendors to maintain and/or improve their good reputation by providing quality products and reliable services to buyers. Laferrière and Décary-Hétu (2023) examined trust signals on darknet single vendor shops, finding that vendors involved in different illicit businesses used different types of trust signals to varying extent. Regarding drug vendors, they found that these vendors displayed more trust signals that described their experience, their illicit business (e.g., providing information about their shop, its management, the goods and services offered, and their quality) and buyer security than vendors of other illegal goods and services.

Because DNMs are zero-trust, high-risk environments, signaling theory is particularly relevant to understanding the signals used to communicate vendor attributes in this environment. According to Ndofor and Levitas (2004), "signaling environment[s] [that] play . . . a key role in determining which signal to use." DNMs can be considered s*ignaling environments*, because administrators of DNMs determine which signals are built into their platform (e.g., escrow systems and feedback mechanisms), with the exception of the language in feedback, vendor profiles, and product listings and descriptions. DNMs escrow systems are used to signal and generate trust between vendors and buyers in low-trust environments (Lorenzo-Dus & Di Cristofaro, 2018; Lusthaus, 2012; Tzanetakis et al., 2016). DNM feedback systems are designed to incentivize vendors to follow through with transactions, foster behavior that meets platform rules and guidelines, and facilitate transactions on the platform to the satisfaction of buyers and sellers (Barratt & Aldridge, 2016; Martin, 2014). DNM discussion forums[1] are also used to build trust, as they include discussions and assessments of vendors to inform other community members of their experiences with vendors (Lorenzo-Dus & Di Cristofaro, 2018). Since the publication of studies on signaling theory, DNMs have added other features to their sites (beyond, for example, feedback and escrow systems) that signal various positive or negative vendor attributes to the buyers to assist the buyers in assessing the trustworthiness of vendors.

Vendor trustworthiness is a concern for DNM members (see, e.g., study on Silk Road user experiences, Van Hout & Bingham, 2013). On the Silk Road DNM, vendors

were considered "trusted sources" following repeated transactions on Silk Road (Van Hout & Bingham, 2013). Kamphausen and Werse (2019) observed that DNM site vendor rating systems as well as vendor discussion forum threads played principal roles in the gaining or loss of vendor trust (p. 283). Another study, which measured vendor's trustworthiness using the cumulative reputation score found on one DNM site, found that "vendor trustworthiness is a better predictor of vendor selection than product diversity or affordability" on the platform (Duxbury & Haynie, 2018). However, there are many other indicators of trust that remain understudied.

There are even fewer studies that have focused on fentanyl trafficking on DNMs (e.g., Ball et al., 2021; Broadhurst et al., 2021) and no mixed method studies that have focused specifically on trust signals in DNM fentanyl networks. Today, fentanyl is banned on most DNMs—at least within the DNM site's community guidelines/rules (e.g., under "Prohibited Items" the Versus DNM site listed "trading of fentanyl or any of its analogues or product containing fentanyl or any of its analogues"). Nevertheless, as Broadhurst et al. (2020) had observed in their study of fentanyl on DNMs in 2019, Dream Market had a similar ban, and yet the researchers were able to identify 48 unique listings of fentanyl on this site (p. 7). Today, there are fewer overt unique listings of fentanyl on DNMs due to increased law enforcement attention on the illegal fentanyl trade. Instead, predominantly, code words for fentanyl are used in lieu of the use of the word "fentanyl" or "fent" (see DEA, 2018), the DNM does not allow categories and subcategories to be created with fentanyl listed, and/or DNM site search functions filter out direct searches of "fentanyl" or "fent." However, this does not necessarily mean that there is less fentanyl sold on DNMs. In fact, fentanyl is still sold on DNM sites, but in more of a clandestine manner, where specific words are used to signal the sale of fentanyl and its quality. Our research seeks to fill the gap in available literature, by identifying the breadth of signals on DNMs that are used to indicate the sale of fentanyl and assess fentanyl vendor trustworthiness, including signals that are provided by the *signaling environment* (i.e., the DNM site through its features) and those provided by the buyers and vendors.

Research Design, Data, Sampling, and Methods

Over the years, DNMs have received increased attention from both scholars and practitioners (e.g., Broadhurst et al., 2021; Lorenzo-Dus & Di Cristofaro, 2018). Our study seeks to expand upon existing DNM research by asking understudied questions and applying mixed methods design. More specifically, our goal here is to show how a mixed methods design can be used in the development of a DNM vendor trustworthiness index. We chose this design because it is often used to provide rich insight into emerging criminal environments, actors, and crimes that cannot be fully understood by using a single-method design (Johnson et al., 2007). First, our mixed methods research is motivated by the following questions: In general, how does one build, maintain, or lose trust in an online environment? What are signals of trust on DNMs? Which features of DNMs are a better indicator of vendor trustworthiness than buyer feedback? What language is used by fentanyl vendors to signal trust? What is the role of trust

when buying and/or selling fentanyl online? Second, we combine quantitative and qualitative research techniques into a single study for the purpose of providing in-depth analyses of our research questions and corroborating information. Specifically, we applied an embedded (or nested) mixed method, which is used when either quantitative or qualitative data are essential to the study and one of these forms of data only provides a supportive, complementary role to the study (Creswell et al., 2003).

In our study, qualitative methods are dominant because of the clandestine nature of the sale of fentanyl on DNMs. In the few fentanyl listings that are available on certain sites (e.g., ASAP and Cartel), fentanyl is not listed in the categories and subcategories of drugs and cannot be found using the search feature of the site (see "Literature Review" section). Researchers need to read vendor descriptions and product listings and buyers' feedback and identify code words used in them to determine if fentanyl is bought and sold. In view of that, our study predominantly relies on qualitative content analysis to identify if fentanyl is sold *and* to identify trustworthiness signals in the text of the vendor descriptions, product listings and descriptions, and buyers' feedback. Quantitative methods are secondary in our study. We embedded it into our research design to enrich our findings and because specific research questions could only be answered by using quantitative methods.

Quantitative methods were applied within one of the several stages in our research: the content analysis of DNMs. Preceding this, we conducted expert interviews and a focus group, desk research and analyses of historic DNM sites, and scraped data from DNMs. Each of the four stages of our mixed-methods study, which is explored below, informs the development of a vendor trustworthiness index.

Expert Interviews and Focus Group Discussion

In this study, we first conducted expert interviews and ran a focus group with criminal justice experts who had extensive experience in conducting darknet investigations of drug trafficking (e.g., Federal Bureau of Investigation, Drug Enforcement Administration, and National Cyber-Forensics and Training Alliance). The main aims for the interviews and the focus group were to: (a) verify and substantiate the information we obtained about DNMs and networks from our own desk research (see next section); (b) identify the top darknet sites where drugs, specifically fentanyl, was bought and sold; and (c) better understand the structure of the darknet drug networks and interactions between DNM buyers and vendors. For this research project, we wanted to ensure that we have the most prominent sites. We did not want to pre-select DNMs because they frequently close (or are shut down) as a result of scam markets (e.g., Sheep, Atlantis, and Evolution) or cyber-dependent crimes committed by other criminals; security concerns and/or concerns over law enforcement attention (e.g., BlackMarketReloaded and Agora); or seizure by criminal justice agencies (e.g., Silk Road, Silk Road 2.0, and Pandora) (Maras, 2017). We also wanted to understand challenges criminal justice agents experience when focusing on illicit DNM transactions.

We used both purposive and snowball sampling to identify experts on the topic of the study. It was not an easy task to locate experts in this field for various reasons (e.g.,

limited expertise and COVID-19 limitations for face-to-face interactions). Nevertheless, we recruited five experts for the in-depth interviews and two for the focus group. While ideally, we wanted more participants, we quickly reached a saturation point and the information we were receiving was somewhat repetitive and confirmed many of our initial findings.

The expert interviews and the focus group were primarily qualitative in nature (open-ended questions). The questions were structured/grouped around a few main themes (e.g., background of interviewees, darknet sites, quantity and quality of drug listings, drug paraphernalia, networks, and trust), including general questions (e.g., "How important is trust on DNMs? In your opinion, how do sellers/vendors attain and maintain trust on these platforms?") to more focused questions (e.g., "Which words are used in drug listings, comments, and reviewers of listings to describe/signal the trustworthiness of sellers?"; "How do we determine key (market) players in these [i.e., DNM] networks?"). The experts, among other things, also guided us in slight modifications to our technical research design. The interviews and focus group ran for approximately 60 min and 120 min, respectively. Instead of audio recordings, three or four team members took detailed notes, which were carefully examined by the research team. Next, this information was analyzed and cross-checked for consistency and then combined into single answers. We did not use content analysis software for the interview and focus group data since their purpose was merely to collect specific DNM-related information and cross-check the information we already gathered through desk research.

Desk Research and Analysis of Historic DNM Sites

Around the time we were preparing our questionnaires and started recruiting subjects for our interviews and focus group, we conducted desk research on DNMs, which included careful analysis of government reports, newspaper articles, academic literature, online forums, and other types of literature. The goal was to gain a better understanding of the way DNMs operate and why they persist in highly uncertain environments. We also wanted to learn about the structure of darknet drug networks and more specifically about the relationships and interactions between buyers and vendors on these sites. This background research helped us better understand the online environment in which these criminal networks flourish and operate.

We conducted thorough reviews of historical sites, including products, discussion forums, posts, vendor ratings, and other items associated with these sites. Specifically, we downloaded and reviewed publicly available archival data of DNM scrapes (Branwen et al., 2015), particularly the now defunct Silk Road, Silk Road 2.0, Pandora, Middle Earth, Agora, and AlphaBay DNMs. This was a very time-consuming task, but it provided the team with comprehensive information about the operations of these sites, the common vocabulary used, and even helped us identify knowledge sharing of DNMs virtual communities of practice with respect to operational security and illicit goods and services on these sites (for the latter, see Maras et al., 2022). The interviews

and the focus group combined with our desk research helped us build the foundation for the scraping of DNMs and content analysis of active DNMs at the time of our data collection.

Scraping Darknet Sites

The data used in this research project were collected from select DNMs operational from 2020 to 2022. Although some minor differences existed in implementing the collection and parsing process for data collected from the different DNMs, they followed the same general process, which included five steps: (a) site access and account creation, (b) site reconnaissance, (c) category page collection, (d) vendor profile page collection, and (e) product page collection.

Before starting the data collection process for the sites selected, each site was accessed via the Tor browser (many DNMs can also be accessed using I2P or Freenet). Once accessed, a customer account for the DNM is created, which allows full access to the site's front end. Generally, it is good practice to allow a period of time to elapse between account creation and data collection. We waited a week before collecting data from the sites to bypass automatic abuse protection on the sites by allowing some time to pass between creation of the account and the large-scale access to the site that is required for scraping. During the period between creating the customer account and the data collection phase, reconnaissance is conducted to identify the captcha system used, the login process for the DNM, and the data available on the category, product, and vendor pages. While manually examining the site during reconnaissance, the HTML code of each page type (categories, vendors, and products) is directly accessed using a browser's "view HTML source" feature, examined, and then mapped into actionable intelligence fields. It is during this phase that we make decisions about what data will be collected during the data collection (i.e., web scraping) process.

Once the general structure of the site is identified, adjustments can be made to the category page, vendor page, and product page collection programs to optimally collect the data in a way it can be best stored in a database for analysis. These adjustments ensure the collection process is optimized to collect the maximum amount of data by visiting the minimum number of pages. This optimization is demonstrated by our exclusion from the collection process of vendor storefront data, which can be recreated by combining the vendor profile data and the product/category data.

Finally, we utilize the system in a manner that would trigger the captcha or marketplace's security system to determine the most effective method of incorporating their inevitable activation into the data collection code. It is critical that we attempt to understand operational security issues and what data collection behaviors will trigger scrutiny from site administrators, as these site administrators have the ability to blacklist the account we use to access the site, or even in some cases (when it comes to clearnet servers) our IP address. DNM site administrators also frequently use login timeouts to automatically logout user accounts, making scraping a more difficult task (Ball et al., 2021, p. 17) In addition, it is critical not to accidentally perform a

denial-of-service attack on the DNM by flooding the server with too many requests at once (Alhatib & Basheer, 2019, p. 56).

A custom javascript web scraping program was written to automatically access each page of the DNM. The scraped data are first stored in text files; once parsed, it is converted into CSV files. These CSV files can later be turned into a more robust database for analysis (Ball et al., 2021, pp. 9–13). The category pages are the first type of DNM pages collected. First, the smallest number of categories required to collect all the accessible product listings are identified. A search criterion is then implemented to return the maximum number of products per page for each marketplace. The program starts when each category's seed page (starting page) is provided. Once each category page is accessed, the vendor profile page URLs, product page URLs, and other category page URLs are extracted from the site's HTML code. The site is automatically examined for all URL hyperlinks present on the page and indexed. If an extracted URL has not been previously collected, it is added to a data set containing all the unique URLs collected from the category pages. A filter is placed in the category data collection program to ensure that only URL links matching the category URL pattern are accessed during the collection of category data. When the program accesses a page, two files are created: (a) a text file containing the HTML code of the page and (b) an image file containing a screenshot of the HTML page displayed in a browser. Once the program has accessed all the available category pages, the URLs stored in the set are added to a text file. The URLs stored in this text file will be used to collect the vendor and product pages on the DNM.

The next phase of data collection involves collecting the vendor pages. Each URL collected during the collection of the category page is examined individually to determine if it matches the pattern of a vendor page URL. Each URL is then added to a native set variable. The set data type is utilized to take advantage of its unique ability to filter and reject duplicate variables from being added to the set. This allows the program to only visit any URL once and in cases when additional URLs need to be collected while collecting the vendor profile URLs, duplicate data will not be added to the set. In addition to the use of the set data type, a filter is utilized to ensure that vendor profile URLs are added to the set. The program then accesses each vendor profile stored in the set and terminates when the last URL stored in the set has been accessed by the program. Similar to the collection of the category pages, the HTML data is stored in a text file, while a screenshot of the page loaded in the browser is stored. If the DNM stores all the vendor information on a single page, only the URLs in the set are visited. If multiple HTML pages are used (PGP Key and vendor feedback), additional URLs are collected from the vendor pages visited.

The URLs extracted during this process are added to the end of the set, and a text file containing these newly collected URLs. This preventive measure ensures that if the program terminates unexpectedly or due to connection or site availability issues, the program can recreate the set in the order initially implemented. An additional text file is used to keep track of the last URL accessed. If there is a problem with the collection (i.e., a dropped connection, a security lockout, a login timeout, etc.), the program is restarted using the URLs already collected and accessed. The program can

then restart scraping where it left off. The program can then go through the URLs and identify the URL last accessed and continue the scraping. Once all the vendor URLs have been accessed, and the collection of the vendor pages is complete, the data stored in the vendor URL set is placed in a text file. Finally, the product URLs are placed in a set and accessed. The data from each product page accessed are stored in text and image files using the same process for collecting category and vendor pages. Additional pages are not extracted from the product page since any additional data present on these pages is also stored on a category and vendor page associated with the product page. Like the vendor page, a record is kept of the current URL being accessed to allow the program to be restarted and resume collection from the last URL accessed.

Before starting the data parsing phase, a data dictionary is developed to determine the variables available for collection on the category, vendor, and product HTML pages. The HTML code and the data displayed in a web browser are examined to determine an exhaustive list of available data variables. Once the variables are identified, appropriate labels are chosen to ensure that the data remains meaningful while remaining universal enough to allow the data dictionary to be used for multiple DNMs. A description and an example of each data variable were placed in the data dictionary. Two researchers collected and labeled the data to ensure that all data variables were collected, and the appropriate examples, labels, and descriptions were created for the data dictionary. It is our experience that all the relevant data should be identified both as displayed in a web browser and written in an HTML page. The researchers independently created their list of labels and examples. The lists were then compared for discrepancies and adjusted after discussion regarding each researcher's criteria for the use of a particular label and the selection of a particular example. Regular expressions were coded using the data dictionary to extract each data variable added to the data dictionary. Once the regular expressions are created, the first data extraction was performed. Based on the results of the first collection, the regular expressions were adjusted to ensure that the program is collecting all the available data on the HTML pages accurately. The collected data are stored in CSV files and added to a database that is used during the content analysis phase of the research.

Content Analysis of DNMs

Following the scraping of selected DNMs and the creation of our database, both qualitative (dominant) and quantitative (supportive) content analyses of the DNM site data were conducted. One of the main reasons for mixing and embedding the methods at this stage is that although some questions could be answered quantitatively most questions required a qualitative response.

We analyzed data from four DNMs (i.e., Vice City, Versus, Cartel, and ASAP), which were top markets identified by criminal justice experts and our desk research at the time of our data collection. At this stage of the project, we took an embedded mixed methods approach, since four active DNMs were studied in depth, integrating them into a larger qualitative study. We then reviewed the data and created a codebook (of variables) based on the coding protocol we developed. Our codebook included

monikers, PGP keys, products, category of products, price of product, amount per sale quantity, quantity available for sale, date vendor registered for the site, date last active on the site, vendor description, product description, various vendor ratings and scores, and the feedback message, type, score, and listing, among other items. In our codebook, we included all DNM-specific signals that could be used to assess vendor trustworthiness.

We used Python and Atlas.Ti to analyze the variables we identified in the codebook and its associated data. First, Python was used. Python regular expressions were coded using the data dictionary to extract each data variable added to the data dictionary. Once the regular expressions were created, the first data extraction was performed using Python. Based on the results of the first collection, the regular expressions were adjusted to ensure that the program collected all the available data on the HTML pages accurately. During the parsing process, different types of content analysis were performed on the content of each page parsed. For example, since the study focused on fentanyl, regular expressions were developed to indicate vendors' overt sale of fentanyl. More specifically, if the term "fent" or "fentanyl" (or words relating to fentanyl analogs, such as "carfentanil" or "carf") was identified on the HTML page, a Boolean term was added to the table containing the extracted data to indicate an overt fentanyl listing. The focus group and interviews, along with desk research, also enabled us to develop a list of explicit covert fentanyl terms (e.g., "M30," "blues," and "pressed") to signal that the product is fentanyl, a fentanyl derivative product or product that contains fentanyl. During our research, we further identified semi-covert words used to refer to fentanyl (including brand names for fentanyl; we accounted for misspelling of words). For example, on ASAP, we observed a listing for Abstral, which is the brand name for sublingual fentanyl (it was misspelled in the listing: "Abstrall 800mg Sandoz pills"). These terms, when identified within a HTML page, were linked to a vendor and listing, and added to the table by the python program during the parsing phase. As a quality check for each result that contained one or more of the code words, we reviewed each result (a very time-consuming task but necessary task to ensure that the listing was signaling the sale of fentanyl—particularly in cases that did not overtly list this illicit drug). Overall, we identified overt, semi-covert, and covert fentanyl listings on the DNMs we reviewed. Unlike previous studies (Broadhurst et al., 2020), we identified few overt unique fentanyl listings and vendors selling fentanyl (specifically, on ASAP and Cartel) (see Table 1, for an illustration of the few listings and difficulty in identifying fentanyl) and we were able to identify semi-covert and/or covert fentanyl listings on all four sites (ASAP, Cartel, Versus and Vice City) (see Table 2 for examples).

Second, Atlas.Ti, a form of computer-assisted qualitative data analysis software (CAQDAS), is used for data visualization and to conduct content analysis of the dataset. This software is used to predominantly conduct qualitative research to identify buyers' sentiments (e.g., positive and negative feedback of vendors and products), understand buyers' feedback about vendors and their goods and services, and identify trust signals in vendor's profiles and product descriptions. The data are sorted, grouped, and analyzed together to identify any common themes that emerge from this dataset.

Table 1. Overt Fentanyl Signals on DNMs.

DNMs	ASAP	Cartel	Versus[2]	Vice City
Total number of overt fentanyl signals on category listing pages	11	8	0	0
Total number of overt fentanyl signals on product pages	5	9	0	0
Total number of overt fentanyl signals on vendor profile pages	1	0	1	0
Total number of overt fentanyl listings	11	17	1	0
Total number of overt fentanyl vendors	7	10	1	0
Total number of overt fentanyl confirmed sales (feedback)	8	15	0	0
Total number of overt fentanyl signals found on DNM	26	32	1	0

Note. DNM = darknet markets.

For example, to assess the trustworthiness of a vendor we analyzed and coded the language used in buyers' feedback on the vendor, as well as the language used in the vendor profiles and product descriptions. This qualitative data was supplemented by quantitative data, such as the number of vendor sales on a specific DNM and other DNMs, vendor feedback scores, and vendor ratings (see Table 3). To ensure intercoder reliability, Atlas.Ti data were coded separately, and then we reviewed and discussed coding to verify consistency in coding and resolve any disagreements between coders.

This software was used to conduct both qualitative and quantitative content analysis of the DNM data based on the identified variables in our codebook that signal vendor trustworthiness. In our dataset, we examined the *signaler* (vendor), *receiver* (buyer), the *signal* itself, and the *feedback* (from the receiver to the signaler) on DNMs. In line with existing literature (Ndofor & Levitas, 2004), we observed that the DNMs (i.e., the signaling environments) determined which signals are present on their platforms, except for the language in feedback, vendor profiles, and product listings. We analyzed the DNMs' signals and identified and grouped words and phrases (e.g., "good," "great," "fantastic," "awesome," "poor," "reliable," "good stealth," "good stuff," "great quality," "as described," "buy again") that signaled vendor trustworthiness in the language of profiles, product descriptions, and buyer feedback. For instance, on Cartel, a buyer who purchased fentanyl powder left feedback that included the words and phrases: "'perfect+++ "Best fent ever!," "highly recommend," "just the purest,"" among other words and phrases (see Table 2). We observed that DNM platforms contained signals that provided DNM users with information about vendors' activities, and quantitative and qualitative assessment features (e.g., ratings, rankings, number of reviews, and types of reviews), as well as qualitative and quantitative indicators of the vendor trustworthiness provided by buyers (i.e., from their feedback) and vendors (i.e., from data, e.g., number of sales, and words and phrases in their profiles

Table 2. Examples of Trust Signals on DNMs.

Fentanyl/positive test feedback/exit scam seller

Marketplace	Listing (title)	Transaction rating	Indicators from feedback messages	Vendor rating/ sales
Cartel	Fentanyl powder	Good	"perfect+++," "potency exactly as advertise," "As expected," "Best fent ever!," "more than anticipated," "highly recommend," "Fast shipping," "chatted with this vendor," "just the purest"	5/5 (7)
Cartel	Fentanyl powder 99% pure	Bad	"Ordered over a month ago and still have not received any refunds or reships. If he makes it right then I'll change it but as of right now I'm out 700 bucks"	4.82/5 (22)
Versus	25 × Oxycodone 30MG M30 USA to USA	1/5	"ad states there's never any F in his Oxy, getting a suspicious F reading on a test strip"	4.83/5 (360)
Versus	10 × China White Heroine #4 Uncut	4/5	"FENT WARNING! Energy control tested this, this product contains no heroin; The active ingredients are Tramadol, Fentanyl (19%) and 4-Anilino-N-Phenethyl-Piperidine (aka ANPP, basically another fentalog)," "It has no properties of pure heroin which I have had in the past from different vendors, this is not China white, it's fent!!"	4.67/5 (300)

(Continued)

Table 2. (Continued)

Fentanyl covert and overt listings				
Marketplace	**Listing (title)**	**Listing amount sold/ available**	**Overt/covert indicator of fentanyl**	**Vendor rating/ sales**
Versus	m30 oxycodone blues ×50 pressed	18 (9979)	"blues, pressed"	4.83/5 (128)
Versus	25 × Oxycodone M30 Pressed	0 (99999)	"M30, Pressed"	5/5 (34)
Vice City	OXYCODONE 30mg (M30) Pressed Top Quality	8 (data unavailable)	"M30, Pressed"	98/100 (31)
Vice City	Best pressed m30's on the web come try it! 5 x $80	3 (data unavailable)	"m30, Pressed"	97/100 (136)
ASAP	1× FENTANYL PATCHES 100MG AUROBINDO/ SANDOZ/ TEVA/ CENTRAFARM BAND AIDS	0 (data unavailable)	"FENTANYL"	17/18 (52)
ASAP	FENTANYL PATCHES 10MMCG	0 (7,000)	"FENTANYL"	0 (0)
Cartel	Fentanyl powder 99% pure	8 (data unavailable)	"Fentanyl"	4.82/5 (22)
Cartel	0.5g × carfentanil	0 (data unavailable)	"carfentanil"	None (0)

Note. DNM = darknet markets.

and product descriptions; see some examples of our study's DNM platforms' signals in Table 2).

Scholars conducting research in this area have typically studied trust signals of feedback and rating scores quantitatively. This quantitative assessment shows the number of positive and negative scores vendors have, which is an important variable in determining a vendor's trustworthiness. Other relevant variables that can be studied quantitatively include, for example, the total number of transactions completed by

Table 3. Vendor Trustworthiness Index.

Username Unique name for a specific user on a specific marketplace [Vice City, Versus, Cartel, and ASAP]	*Vendor PGP key* User-generated cypher which allows users to verify their identity [Vice City, Versus, Cartel, and ASAP]	*Registered on* Date member first registered [Vice City, Versus, Cartel, and ASAP]	*Last active* Date member last logged into the site [Vice City, Versus, Cartel, and ASAP]	*Finalize early* Vendors preferred payment before shipping and buyer's receipt of the item [Vice City, Cartel, and ASAP]
Vendor description Vendor-generated content about themselves, the goods and services they provide, current and previous DNM affiliations, and process for purchasing and shipping items to customers, among other things [Vice City, Versus, Cartel, and ASAP]	*Market vendor sales* Total number of transactions completed by vendor on the marketplace [Vice City, Versus, Cartel, and ASAP]	*Market feedback total score* Total feedback generated by the sum of the positive and negative transactions [Vice City, Cartel, and ASAP]	*Market feedback positive/ negative score* Total positive and total negative feedback for a specific vendor given by buyers who purchased items [Versus, Cartel, and ASAP]	*Market vendor rating* Feedback given to the vendor by buyers who purchased item (e.g., positive or negative) [Vice City and Cartel]
Product description Full description about the product and the vendor's rules relating to the purchase of the product [Vice City, Versus, Cartel, and ASAP]	*Other market vendor sales* Total number of transactions completed by vendor on other marketplaces [Vice City, Cartel, and ASAP]	*Other market feedback total score* Total feedback imported from other marketplaces generally including positive and negative feedback [Vice City, Cartel, and ASAP]	*Other feedback positive/ negative score* Total positive and total negative feedback for a specific vendor given by buyers who purchased items on another marketplace [Vice City, Cartel, and ASAP]	*Other market vendor rating* Five-star scale rating imported from another marketplace for a specific vendor given by buyers on another marketplace [Vice City, Cartel, and ASAP]
Quantity available for sale The amount of a specific product the vendor currently has available [Vice City, Versus, Cartel, and ASAP]	*Feedback listing* The vendor listing the buyer provide feedback/ reviewed [Vice City, Versus, Cartel, and ASAP]	*Feedback date* Date feedback was given [Vice City, Versus, Cartel, and ASAP]	*Feedback message* Message left by member who purchased item from specific vendor [Vice City, Versus, Cartel, and ASAP]	*Feedback type/rating* Rating of the vendor (i.e., positive/negative or 0-100) [Vice City, Versus, Cartel, and ASAP]

Note. DNM = darknet markets.

vendors on other markets, the time the vendor has been on a specific site, the amount of a specific product the vendor currently has available, and total vendor sales (see Table 3). Such quantitative approaches, although very useful, are unable to identify underlying meanings of complex phenomena and cannot explain how people interpret the actions of others (Blaikie, 2007).

Recognizing the limitations of quantitative approaches, our research added a strong qualitative component to our study that included, for example, exploration of the unique language used by vendors in their product descriptions; feedback that is not necessarily positive or negative (i.e., neutral); language used to justify specific type of feedback that could only be studied by carefully reviewing the written comments rather than just looking at scores or number of listings and sales; specific monikers and images vendors select when creating their profiles; vendor-generated content about themselves in profiles; and the process for purchasing and shipping items to customers (included in profile description and/or product listings), among other things. This qualitative approach is more interpretative and accepts that the data to be studied/explored contain levels of nuances that may be very difficult to codify in preselected choices.

For our qualitative analysis, we created network diagrams between vendors and buyers[3] to identify and assess relationships between them based on the language analyzed and main themes identified; mapped vendors to the frequency of the use of "positive" and "negative" words and phrases used to describe them; and compared the words and phrases used in vendor profiles and product descriptions to signal trust to the language used in feedback to describe the vendor and the vendor's process and products (e.g., if vendors delivered products as described, buyers were willing to finalize transactions early). We combined these data with quantitative data about ratings, rankings, number of sales, vendors' time active on DNM sites, among other data.

The mix of quantitative and qualitative content analysis of each DNM helped us understand the relationship between our identified variables; this was necessary to develop the first version of the vendor trustworthiness index, which includes all four DNMs—ASAP, Cartel, Versus, and Vice City—to show the functionality of the index (see Table 3). This analysis also provided us with contextual information about the drug markets (including fentanyl markets), as well as the vendors and buyers in these markets. By studying the feedback and vendors' profiles and product descriptions, we gleaned insights about vendors and trust signals. Thus, at the integration stage of this study our qualitative and quantitative findings are analyzed separately and then combined, mainly to provide a more holistic picture of DNM vendor trustworthiness as well as to corroborate and compare information and findings with available research and the information we obtained from criminal justice agents during our expert interviews and focus group.

In this multistage mixed methods study, after the trustworthiness index is finalized, a second round of expert interviews and a focus group with criminal justice experts is run to discuss our trustworthiness index scores. Once again, purposive and snowball sampling is used to identify experts for the focus group. The feedback provided will be taken into consideration in case the experts identify flaws in the trustworthiness index.

We will modify and assess the trustworthiness index accordingly. Ultimately, in our study, the data from the different stages of our research are integrated and combined to show the complexities of the topic of our study, and to ensure that the final product is as complete and as accurate as possible.

Design and Data Limitations and Future Research

While developing our vendor trustworthiness index, we encountered some challenges. There are five main limitations of this research. First, during the focus group and interview stages of our research, we tried to connect with numerous experts in the field from several criminal justice agencies, but this task proved to be challenging since the expertise in this field is limited.

Second, there are many methodologies that can be used to scrape the darknet. These methodologies can differ in important ways and can meaningfully affect the results of the study (Owenson et al., 2018, p. 17). For example, a limitation of data scraping is that data will only be collected if it is available on the DNM at the time of the scraping. DNM pages and data that were present on the site, but removed or altered prior to scraping, or altered between scrapings, will not be available for the program to index. Researchers need to decide how often their systems scrape each individual site. Daily collection is certainly possible and a preferred method but is resource intensive and may trigger security measures on the site being indexed. To mitigate the resource-intensive nature of daily collection, some researchers have used weekly or even monthly snapshots of DNM sites in their entirety (Soska & Christin, 2015). However, as Ball et al. (2021) pointed out, we currently lack an accepted, reliable, and consistent method for capturing DNM data.

Third, DNM scrapes can occur by scraping the actual DNM site or scraping sites that index DNM sites (e.g., Kilos). The advantage to scraping the actual DNM site is the ability to access the entirety of information on the site, in its most raw form. This method may be the most complete method of scraping DNMs. However, due to differences in the architecture of each site, researchers will have to customize their program and scraping techniques for each specific DNM site. This challenge can be overcome by scraping data off sites that index many DNM sites and combine them into a single searchable site. Scraping these index sites may be more time efficient, as the index site creates uniformed data fields between different DNMs. The limitation of scraping index sites is that you only have access to the data that the index site chooses to index on their site. Even if researchers chose to directly scrape individual DNM sites for a more complete dataset, index sites may still be useful to assist the researchers in identifying new DNM sites as they are launched.

Fourth, private communications between DNM members (i.e., buyers and vendors), including potential private drug offerings between users, are not public and cannot be indexed for analysis. This presents a significant limitation of this method, as it is impossible to understand the full scope of DNM drug trades, since we cannot understand or measure the prevalence or frequency of private offerings in direct messages that are facilitated by the DNM. We also cannot identify if the transactions that

are successful on DNMs are influenced in whole or in part by these private transactions and if further communications occur between vendor and buyers, which may influence vendor trustworthiness assessments.

Finally, DNMs are shaped by the need for secrecy. For this reason, it may not always be easy to identify trustworthiness indicators (which also fluctuate between DNM sites). Accordingly, for our research, we used a comprehensive qualitative approach to carefully analyze the language, images, and other signals that vendors and buyers use, which is very time consuming. When conducting such analyses, researchers should acknowledge the limitations of this approach, which tends to be more subjective since researchers interpret the findings/results and the process may be influenced by the personal biases of the researchers. In view of that, more than one researcher should evaluate the data to cross-check observations and findings.

Conclusion

In this article, we presented the research design and methods, we applied to develop a DNM vendor trustworthiness index, identified a range of indicators of trustworthiness of vendors on darknet sites, and discussed limitations relating to this type of research and issues researchers face when studying the complexities of DNMs. Our work has theoretical and practical implications for understanding the role of previously understudied signals of trust in uncertain environments and how trust contributes to the sustainability and growth of illicit DNMs. An important contribution of this article is to show how embedded mixed methods can be used to study DNMs. Although there is a lot of discussion about the benefits of mixed research designs, there is a lack of guidance on the implementation of mixed method research design strategies, particularly in darknet research. In view of that, we provide a detailed guide for developing a vendor trustworthiness index using a mixed methods approach. This approach enriches our understanding of DNMs and actors operating within these spaces because it provides a more holistic view of the topic studied and enables researchers to explore this emerging and understudied topic. Although our study focused on illicit fentanyl vendors, the trustworthiness index can be used to study vendors of other illicit goods and services (e.g., firearms, hacking services, and counterfeit money, documents, and goods, etc.).

The long-term goal of our research project is to use the vendor trustworthiness index in the development of a tool that can identify and map the structure of darknet fentanyl drug markets and interactions between buyers and vendors of fentanyl (and its derivatives and analogs), as well as provide trustworthiness assessments of DNM vendors. This tool can reduce the amount of time and minimize the human, technical, and financial resources needed to conduct these assessments. Ultimately, our work provides researchers and practitioners with the information and tools they need to keep pace with these dynamic markets.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was supported by the U.S. National Institute of Justice [2019-R2-CX-0018].

Notes

1. Note: not every DNM site has built-in discussion forums.
2. On Versus, fentanyl patches were mentioned in the vendor description for shipment by one vendor, another vendor did not offer the sale of fentanyl and carfentanil but sold a fentanyl synthesis guide and a carfentanyl [sic] synthesis guide.
3. Monikers are masked through pseudonymization to protect the confidentiality of the data. We replace the monikers with artificial identifiers and sequential numbers (e.g., Buyer 1, Vendor 1). Note: On DNMs, buyer monikers already have all but their first and last character or number replaced with *. The presentation, analysis, and discussion of the network diagrams are beyond the scope of this article.

References

Alhatib, B., & Basheer, R. (2019). Crawling the dark web: A conceptual perspective, challenges and implementation. *Journal of Digital Information Management*, *17*(2), 55–56.

Bakken, S. A. (2021). Drug dealers gone digital: Using signaling theory to analyse criminal online personas and trust. *Global Crime*, *22*(1), 51–73. https://doi.org/10.1080/17440572.2020.1806826

Ball, M., Broadhurst, R., Niven, A., & Trivedi, H. (2021). *Data capture & analysis of darknet markets* (Working Paper). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3344936

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. https://doi.org/10.1016/j.drugpo.2016.07.005

Bird, R. B., & Smith, E. A. (2005). Signaling theory, strategic interaction, and symbolic capital. *Current Anthropology*, *46*, 221–248. https://doi.org/10.1086/427115

Blaikie, N. (2007). *Approaches to social enquiry* (2nd ed.). Polity Press.

Branwen, G., Christin, N., Décary-Hétu, D., Andersen, R. M., StExo, El Presidente, Anonymous, Lau, D., Sohhlz, Kratunov, D., Cakic, V., Buskirk, V., Whom, McKenna, M., & Goode., S. (2015). *Dark net market archives*, 2011–2015. https://gwern.net/dnm-archive

Broadhurst, R., Ball, M., Jiang, C., Wang, J., & Trivedi, H. (2021). *Impact of darknet market seizures on opioid availability* (Research Report 18). Australian Institute of Criminology (AIC).

Broadhurst, R., Ball, M., & Trivedi, H. (2020). *Fentanyl availability on darknet markets* (Australian Institute of Criminology (AIC), Trends & Issues in Crime and Criminal Justice No. 590, February 2020). https://www.aic.gov.au/sites/default/files/2020-05/ti590_fentanyl_availability_on_darknet_markets.pdf

CDC. (2022). *U.S. Overdose deaths in 2021 increased half as much as in 2020—But are still up 15%.* https://www.cdc.gov/nchs/pressroom/nchs_press_releases/2022/202205.htm

Connelly, B. L., Certo, S. T., Ireland, R. D., & Reutzel, C. R. (2011). Signaling theory: A review and assessment. *Journal of Management*, *37*(1), 39–67. https://doi.org/10.1177/014920631038

Creswell, J. W., Plano Clark, V., Gutmann, M., & Hanson, W. (2003). Advanced mixed methods research designs. In A. Tashakkori & C. Teddle (Eds.), *Handbook of mixed methods in social and behavioral research* (pp. 209–240). SAGE.

DEA. (2018). *Slang terms and code words: A reference for law enforcement personnel* (DEA Intelligence Report (DEA-HOU-DIR-022-18)). DEA Houston Division.

DEA. (2021). *2020 national drug threat assessment*. https://www.dea.gov/sites/default/files/2021-02/DIR-008-21%202020%20National%20Drug%20Threat%20Assessment_WEB.pdf

Décary-Hétu, D., & Laferrière, D. (2015). Discrediting vendors in online criminal markets. In G. Bichler & A. E. Malm (Eds.), *Disrupting criminal networks: Network analysis in crime prevention* (pp. 129–152). Lynne Rienner.

Décary-Hétu, D., & Leppänen, A. (2016). Criminals and signals: An assessment of criminal performance in the carding underworld. *Security Journal*, *29*(3), 442–460. https://doi.org/10.1057/sj.2013.39

Duxbury, S. W., & Haynie, D. L. (2018). The network structure of opioid distribution on a darknet cryptomarket. *Journal of Quantitative Criminology*, *34*, 921–941. https://doi.org/10.1007/s10940-017-9359-4

Fischer, E., & Reuber, R. (2007). The good, the bad, and the unfamiliar: The challenges of reputation formation facing new firms. *Entrepreneurship Theory and Practice*, *31*, 53–75. https://doi.org/10.1111/j.1540-6520.2007.00163.x

Gambetta, D. (2009). Signaling. In P. HedstrÖm & P. Bearman (Eds.), *The Oxford handbook of analytical sociology* (pp. 168–194). Oxford University Press.

Hardy, R. A., & Norgaard, J. R. (2016). Reputation in the internet black market: An empirical and theoretical analysis of the deep web. *Journal of Institutional Economics*, *12*(3), 515–539. https://doi.org/10.1017/S1744137415000454

Holt, T. J., Smirnova, O., & Hutchings, A. (2016). Examining signals of trust in criminal markets online. *Journal of Cybersecurity*, *2*(2), 137–145. https://doi.org/10.1093/cybsec/tyw007

Johnson, R. B., Onwuegbuzie, A. J., & Turner, L. A. (2007). Toward a definition of mixed methods research. *Journal of Mixed Methods Research*, *1*(2), 112–133. https://doi.org/10.1177/1558689806298224

Kamphausen, G., & Werse, B. (2019). Digital figurations in the online trade of illicit drugs: A qualitative content analysis of darknet forums. *International Journal of Drug Policy*, *73*, 281–287. https://doi.org/10.1016/j.drugpo.2019.04.011

Kirmani, A., & Rao, A. R. (2000). No pain, no gain: A critical review of the literature on signaling unobservable product quality. *Journal of Marketing*, *64*(2), 66–79. https://journals.sagepub.com/doi/10.1509/jmkg.64.2.66.18000

Laferrière, D., & Décary-Hétu, D. (2023). Examining the uncharted dark web: Trust signaling on single vendor shops. *Deviant Behavior*, *44*, 37–56. https://doi.org/10.1080/01639625.2021.2011479

Lorenzo-Dus, N., & Di Cristofaro, M. (2018). "I know this whole market is based on the trust you put in me and I don't take that lightly": Trust, community and discourse in crypto-drug markets. *Discourse & Communication*, *12*(6), 608–626. https://doi.org/10.1177/1750481318771429

Lusthaus, J. (2012). Trust in the world of cybercrime. *Global Crime*, *13*(2), 71–94. https://doi.org/10.1080/17440572.2012.674183

Maras, M.-H. (2017). *Cybercriminology*. Oxford University Press.

Maras, M.-H., Arsovska, J., Wandt, A., Knieps, M., & Logie, K. (2022). The SECI model and darknet markets: Knowledge creation and sharing in criminal organizations and communities of practice. *European Journal of Criminology*. Advance online publication. https://doi.org/10.1177/14773708221115167

Martin, J. (2014). *Drugs on the dark net: How cryptomarkets are transforming the global trade in illicit drugs*. Palgrave Macmillan.

Maynard-Smith, J., & Harper, D. (1995). Animal signals: Models and terminology. *Journal of Theoretical Biology*, *177*, 305–311. https://doi.org/10.1006/jtbi.1995.0248

Miller, J. (2020). The war on drugs 2.0: Darknet Fentanyl's rise and the effects of regulatory and law enforcement action. *Contemporary Economic Policy*, *38*(2), 246–257. https://doi.org/10.1111/coep.12447

Owenson, G., Cortes, S., & Lewman, A. (2018). The darknet's smaller than we thought: The life cycle of tor hidden services. *Digital Investigation*, *27*, 17–22. https://doi.org/10.1016/j.diin.2018.09.005

Riley, J. C. (2001). Silver signals: Twenty-five years of screening and signaling. *Journal of Economic Literature*, *39*, 432–478.

Soska, K., & Christin, N. (2015). *Measuring the longitudinal evolution of the online anonymous marketplace ecosystem*. Proceedings of 24th USENIX Security Symposium, Washington, DC (August 12-14, 2015). https://www.usenix.org/system/files/sec15-paper-soska-updated_v2.pdf

Spence, M. (1973). Job market signaling. *Quarterly Journal of Economics*, *87*, 355–374. https://doi.org/10.2307/1882010

Spence, M. (2002). Signaling in retrospect and the informational structure of markets. *American Economic Review*, *92*, 434–459. http://www.jstor.org/stable/3083350

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 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. https://doi.org/10.1016/j.drugpo.2013.01.005

Author Biographies

Marie-Helen Maras is an associate professor at the Department of Security, Fire, and Emergency Management and the Director of the Center for Cybercrime Studies at John Jay College of Criminal Justice. She holds a DPhil in Law and an MPhil and MSc in Criminology and Criminal Justice from the University of Oxford. Her academic background and research cover cybersecurity, cybercrime, and the legal, political, social, cultural, and economic impact of digital technology. She is the author of numerous peer-reviewed academic journal articles and books, the most recent of which is *Cybercriminology* (Oxford University Press), and serves as a consultant and subject matter expert on cybercrime and cyber organized crime at the United Nations Office on Drugs and Crime.

Jana Arsovska is an associate professor of sociology at John Jay College of Criminal Justice and the Program of Doctoral Study in Criminal Justice at the Graduate Center, City University of New York. She is a Research Associate at the Center for Cybercrime Studies and the former director of the Master of Arts Degree Program in International Crime & Justice and the Certificate in Transnational Organized Crime at John Jay College. She holds a PhD degree in International Criminology from Leuven University in Belgium where she studied organized crime. She is the recipient of various prestigious grants and awards and has published extensively on organized and transnational crimes.

Adam Scott Wandt is an assistant professor of Public Policy and Vice Chair for Technology of the Department of Public Management at John Jay College of Criminal Justice. He is a member of the graduate faculty in the Master of Public Administration and the Master of Digital Forensics and Cybersecurity programs. Professor Wandt is a practicing Attorney and Counselor-at-Law (New York) and is co-Chair of the New York City Bar Association's Committee on Technology, Cybercrime, and Privacy Law. He has worked on sponsored research for, or in partnership with, the Federal Bureau of Investigation, U.S. Department of Justice, U.S. Bureau of Justice Statistics, Interpol, the United Nations, Sprint, BlackBoard, as well as law enforcement and educational institutions around the world.

Kenji Logie is a third-year student in the Criminal Justice PhD program at John Jay College of Criminal Justice. He has been an adjunct lecturer at CUNY for the last 7 years, teaching courses in programming, database design, digital forensics, and system analysis and design. He holds a BS/MPS in business information systems from Brooklyn College (CUNY), and an MS in digital forensics and cybersecurity from John Jay College of Criminal Justice (CUNY).