Invitation Article

New Directions in Online Illicit Market Research

*Thomas J. Holt, Ph.D.**
Professor
School of Criminal Justice
Michigan State University

Abstract

Criminological scholarship has long examined the ways that illicit goods and services are traded through underground economies, such as narcotics and stolen goods. In the last two decades, researchers have explored the ways that online spaces, such as forums, are used by actors to engage in the sale of digital goods, including stolen personal information and malicious software. Additionally, research has begun to explore the ways that a global network for the sale of drugs has emerged in online markets operating on the so-called Dark Web. Though these studies improve our understanding of the basic social structures that drive online transactions for various criminal services, myriad questions remain as to what drives engagement in online markets and the ways that they persist and evolve over time. This work provides an overview of the various illicit markets operating on the Open and Dark Web, and their relationship to open and closed economically-motivated illicit goods and services markets in the real world. This work also explores the range of research questions that must be addressed to improve our understanding of the actors who shape the processes of online markets, inclusive of buyers, sellers, and website operators.

Keywords

Illicit Markets, Economic Crime, Cybercrime, Cryptomarkets, Dark Web, Drugs, Hacking, Rational Choice

---

* This article is based on Professor Holt's keynote lecture delivered to the International Forum of the Korean Institute of Criminology, Seoul, Korea, on December 3rd, 2020.
* http://dx.doi.org/10.36889/IJCJ.2021.005.
* Direct correspondence to Thomas J. Holt, Ph.D., Professor, School of Criminal Justice, Michigan State University; e-mail: holtt@msu.edu.
INTERNATIONAL JOURNAL OF CRIMINAL JUSTICE, Vol. 3 Issue 1, June 2021, 3-23

NEW DIRECTIONS IN ONLINE ILLICIT MARKET RESEARCH

Criminological scholarship has historically focused on the distribution of a variety of illicit goods and services, ranging from prostitution (e.g. Cunningham & Shah, 2016), drugs (Adler, 1993; Jacobs, 1996; Sterk, 1999; Turnbull, 2002), and weapons (Cook, Cukier, & Krause, 2009; Hureau & Braga, 2018), to more exotic items such as endangered wildlife (Lavorgna, 2014; Sollund, 2019). These studies provided rich insights into not only the practices of buyers, sellers, and market facilitators (Adler, 1993; Jacobs, 1996; Wright & Decker, 1994; 1996), but also into the social and economic factors that influence involvement in illicit exchanges (Cunningham & Shah, 2016; Jacobs, 2000). Scholars have also examined the efficacy of law enforcement efforts to dismantle illicit economies (Eck, 1995; May & Hough, 2004), and the ways that offender behaviors evolve to reduce the risk of arrest (Cross 2000; Jacobs 1996; 2010; Johnson et al. 2000; Johnson & Nataranjan 1995; Knowles 1999; Topalli et al. 2002; VanNostrand & Tewksbury 1999).

In recent years, offenders have seized upon the opportunities afforded by the Internet and mobile devices to expand the scope of illicit market operations (Holt & Bossler, 2015; Mann & Sutton, 1998). The communications, finance, and retail tools available through the World Wide Web and social media application made it possible for illicit markets that traditionally existed in physical spaces to move their operations into virtual spaces (Barratt, 2012; Franklin et al., 2007; Holt et al., 2016; Martin, 2014). In fact, there are now services selling access to sex (Cunningham & Kendall, 2010; Weitzer, 2012), narcotics (Barratt, 2012; Martin, 2014; Moeller et al., 2017; Tzanetakis et al., 2017), counterfeit documents (Holt & Lee, 2020), and even hitmen and contract violence providers (Roddy & Holt, 2020). These activities may be viewed by some as cybercrimes by virtue of the use of technology in the offense, though they may be defined more as cyber-enabled crimes as they can be performed without technology, but are made easier through this medium (Dowling & McGuire, 2013; Holt & Bossler, 2016).

There are also forms of cybercrime that may be referred to as cyber-dependent crimes, like computer hacking, as they cannot be performed without the use of computers and the Internet (Dowling & McGuire, 2013; Holt & Bossler, 2016). Individuals involved in these offenses have created underground economies where

malware, attack services, and access to sensitive data are available on a fee-for-service basis (Dupont et al., 2017; Franklin et al., 2007; Holt, 2012; Holt, 2013; Hutchings & Holt, 2015). Online markets selling email lists for spam campaigns, global distribution of malicious software, and access to stolen credit card numbers emerged in the early 2000s and have evolved in tandem with the applications and services on the Internet (Dupont et al., 2017; Holt & Dupont, 2019; Hutchings & Clayton, 2016; Smirnova & Holt, 2017).

Research exploring the online markets for physical and digital goods has increased dramatically over the last decade, examining aspects of market operations and the utility of some theories to account for these offenses (Holt & Bossler, 2015; Hutchings & Holt, 2017). Though valuable, there is a need for a systematic review of the literature related to online illicit markets to identify gaps in the literature that must be addressed. Such work is essential to improve our fundamental understanding of the participants of markets, whether as vendors, buyers, or facilitators, as well as their technical and social structure. This work will provide an analysis of the state of virtual market research and its operations on both the Open and Dark Web based on the existing body of empirical research. A series of recommendations are provided for future research in the hopes of improving the capacities of policy makers and practitioners in cybersecurity and law enforcement around the world.

DIFFERENTIATING PHYSICAL AND VIRTUAL MARKETS

Criminological and sociological inquiry into the nature of illicit goods markets has been particularly useful to understand the structural distribution models at play for different products and services (Adler, 1993; Jacobs, 1996; Klockars, 1974; Potter, 2009). The dynamics that shape the practices of markets are due in part to the visibility that their illicit exchanges may have to the general public. The most often examined illicit markets are those which occur in relatively public settings, whether in street corners, alleys, or the front porches of homes and apartment buildings as with drug sales (Jacobs 1996; 2000; Johnson, Dunlap, & Torginy 2000; Johnson & Nataranjan 1995; Knowles 1999; Topalli, Wright, & Fornango 2002; VanNostrand & Tewksbury 1999; Weitzer, 2012). Such exchanges are

typically referred to as open markets by virtue of the public visibility of the activities (Eck, 1995; May & Hough, 2004). Involvement in transactions in open markets creates risk for both buyers and sellers, as both parties can be observed by police and other informal agents of social control, such as neighbors or community watch groups (Jacobs, 2010; May & Hough, 2004). In addition, the presence of drugs, weapons, and cash creates a point of risk for market participants from other criminals who would target them for robbery or theft (Gibbs, 1997; Jacobs, 1996, 2010).

Due to the range of risks present in open illicit markets, a portion of actors shifted their practices to reduce the risk of detection (e.g. Gibbs, 1996; May & Hough, 2004). Specifically, sellers began to engage in transactions with only those individuals who they knew or trusted in some way (Johnson et al., 2000; May & Hough, 2004). They also began to operate in low visibility environments, such as in residences or other controlled and enclosed spaces (Hammid, 1998; Johnson et al., 2000; May & Hough, 2004). Some also continued to operate in public spaces, though they dramatically reduced their visibility and vending practices. Such markets came to be known as closed markets due to their restrictions and limited access to outsiders (May & Hough, 2004).

The organization and practices of actors involved in physical illicit markets are replicated to some degree in virtual spaces. Many of the advertisements for illicit products in online spaces operate in a quasi-open state in that they can be identified with relatively little difficulty through search engines or other publicly accessible means (Franklin et al., 2007; Holt & Lampke, 2010; Holt & Lee, 2020; Tzanetsakis et al., 2016; Yip et al., 2013). Additionally, the public statements made by vendors regarding their products and services are similar to open air illicit markets in that they are hawking their wares to any interested parties (Holt & Dupont, 2019; Odabas et al., 2017).

There are minor differences in the operating environments where buyers and sellers congregate online. First, illicit products can be identified for sale via online platforms that can be accessed using a traditional web browser, search engine, and appropriate key terms (Holt & Lampke, 2010; Hutchings & Holt, 2015; Odabas et al., 2017; Yip et al., 2013). This environment is often referred to as the Open Web, in that anyone can access website content through the use of any browser software, and this information may be indexed and retained by search engines and

historical web archives (Smirnova & Holt, 2017).

Various illegal products and services are also readily available on the so-called Dark Web, which is an encrypted portion of the Web that can only be accessed through the use of specialized browser software (Barratt, 2012; Decary-Hetu et al., 2016; Martin, 2014; Smirnova & Holt, 2017). There are various tools that can be used to access the Dark Web, though the most prominent software is called TOR, or The Onion Router, which is a free software program incorporating encryption software with a Firefox browser plugin (Martin, 2014). TOR functions by routing user web traffic through other TOR users' internet connections at multiple points to effectively hide the IP address and information of all within the network (Barratt, 2012). Websites hosted on servers connected to TOR utilize similar processes which makes it exceedingly difficult to identify the physical location of websites to shut down their operations (Decary-Hetu et al., 2016).

Regardless of platform, there are two primary modes of selling products. The first involves the use of single-operator e-commerce style platforms to facilitate transactions. These sites are typically referred to as "shops" as they provide access to various goods and services sold by one individual (Copeland et al., 2020; Holt & Lee, 2020; Smirnova & Holt, 2017). Customers can identify shops through various search engines or links posted on dark web indexes, though they may have to register with the site in order to complete a purchase or see their exact products for sale (Copeland et al., 2020; Holt & Lee, 2020; Smirnova & Holt, 2017). Registration systems vary based on the vendor, but typically require an individual to provide a username and password in order to create an account that can give them access to site content (Holt & Lampke, 2010; Smirnova & Holt, 2017).

The second model involves the use of forum software, which provides an asynchronous communications platform hosted on the websites designed to connect participants from around the world (Dupont et al., 2017; Holt, 2007; Hutchings & Holt, 2015; Mann & Sutton, 1998). Forums comprise an online discussion group with a specific topic focus, segmented by sub-topic (Holt, 2007; Holt & Bossler, 2015; Mann & Sutton, 1998). Conversations begin when an individual makes a post about a specific issue, which in the context of illicit markets involves the products or services they have for sale, or may be seeking. Responses to that

post are threaded together sequentially to provide an ongoing dialogue (Holt, 2007; Holt & Lampke, 2010; Mann & Sutton, 1998).

Forums used to sell illegal good and services have been observed since the early 2000s, and can operate in a similar fashion to a retail mall in physical space (Dupont et al., 2017; Holt & Lampke, 2010; Odabas et al., 2017). The site operators provide a communications space via the forums, and vendors can post ads directly next to their competitors. Customers can then review all advertisements and ask questions about the products, before selecting a vendor with whom to engage in a transaction (Odabas et al., 2017). The actual exchange takes place outside of the forum, though customers can provide reviews of the quality of the vendor and their services within their thread after a transaction is complete (Dupont et al., 2017; Holt & Lampke, 2010; Hutchings & Holt, 2015).

Variants of forums also exist on the Dark Web which are called cyrptomarkets, referencing the notion that the site is hosted on an encrypted portion of the Internet and utilizes encrypted payment methods to facilitate illicit commerce (Barratt, 2012; Decary-Hetu et al., 2017; Moeller et al., 2017). Cryptomarkets can provide a space for multiple vendors to sell products simultaneously, as with forums, though there are some that are single operator shops selling multiple products (Decary-Hetu et al., 2017; Moeller et al., 2017; Tzanetakis et al., 2017).

Forums and cryptomarkets typically require participants to register with the forum in order to post messages, and may also hide posted content from outsiders until they register. Such a practice still fits within the notion of a quasi-open market (Holt & Dupont, 2019), as these sites may be identified on the basis of their involvement in the sale of illicit goods, like stolen credit card data (Decary-Hetu & Leppanen, 2013; Holt & Lampke, 2010), hacking tools (Holt, 2013), or drugs (Decary-Hetu & Gommoni, 2017; Decary-Hetu et al., 2016).

To reduce the risk of registration by law enforcement and the research community, some forums and cryptomarkets have adopted strategies that mirror the characteristics of closed markets in physical space. For instance, some sites require potential participants to pay for access to the market in order to increase the likelihood that they will complete a transaction (Decary-Hetu et al., 2017; Dupont et al., 2017; Holt & Dupont, 2019). Others have adopted social vetting schemes, where anyone who attempts to register with the site are required to

provide details about their involvement in other online communities and illicitactivities (Dupont et al., 2017; Holt & Dupont, 2019; Meyer, 1989). The applications are then reviewed by the existing members who can provide feedback and essentially vouch for the individual's claims (Dupont et al., 2017; Holt & Dupont, 2019).

UNDERSTANDING THE PRACTICES OF PARTICIPANTS IN ONLINE ILLICIT MARKETS

The differences observed in the structure of the forums and shops operating on the Open and Dark Web call to question how participants engage in illicit exchanges online. Research indicates there are substantial similarities in the ways that vendors advertise and engage in transactions (Holt & Lee, 2020; Smirnova & Holt, 2017). The process of beginning a transaction are quite similar, regardless of whether the vendor offers physical goods, such as drugs, or virtual commodities like credit card numbers. Studies utilizing crime script analyses illustrate that vendors must first make their advertisement and provide an overall description of their products, pricing, and purchasing details (Copeland et al., 2020; Decary-Hetu et al., 2016; Holt & Lee, 2020; Hutchings & Holt, 2015; Roddy & Holt, 2020).

Advertisements that provide concise details as to the nature of their products are often seen as being more legitimate, particularly if they can provide photos of the items that are not taken from other websites or stock photos (Copeland et al., 2020; Tzanetakis et al., 2017). Variations in the nature of products also creates differences in the language included in advertisements. For instance, individuals offering stolen credit and debit card information often provide specific details as to the bank that issued the card, and the state and country of origin for the data (Franklin et al., 2007; Holt & Lampke, 2010; Smirnova & Holt, 2017). Vendors selling passports and identity documents often identify the exactpersonal information potential customers need to provide in order to create the document (Holt & Lee, 2020). Sellers may also provide information on their shipping procedures, particularly in the case of firearms and narcotics, so that customers understand how products may arrive (Copeland et al., 2020; Decary-Hetu et al., 2017).

Once an advertisement has been created, customers are then required to reach

out to the vendor to complete a transaction. In the case of forums and cryptomarkets, customers may contact the vendor via private messaging applications or email (Decary-Hetu et al., 2017; Martin et al., 2014). This is also true for some shops on both the open and dark web, which may use website-based contact forms or internal ticketing and communications tools that allow customers to connect with vendors (Copeland et al., 2020; Holt & Lee, 2020; Roddy & Holt, 2020). Vendors are also increasingly using encrypted email systems, like Protonmail, on both the open and dark web as they provide end-to-end protection for the contents of emails in transit (Decary-Hetu et al., 2016; Martin, 2014). Should law enforcement or other entities intercept messages as they move between email servers, it is not possible to read its contents without the decryption key which is available only to the account holder (Decary-Hetu et al., 2016; Martin, 2014). Some services will also not log personal information, including IP address details, reducing the potential for loss of sensitive details to outsiders (Decary-Hetu et al., 2016).

Next, potential customers must attempt to place an order with the vendor through whatever preferred contact method they may indicate. Buyers must be exact in their order, stating the quantity of product and any specifics associated with design or customization, as is the case with fraudulent identity documents (Decary-Hetu et al., 2016; Holt & Lee, 2020; Odabas et al., 2017). It is also possible for customers to negotiate price when purchasing in bulk quantities, or should the vendor allow for discount codes or coupons to reduce the final price (Barratt, 2012; Dupont et al., 2017; Holt & Lampke, 2010; Holt & Lee, 2020; Hutchings & Holt, 2015). The use of discounts is thought to be a way for reputable vendors to retain customers over the long term and provide a degree of customer service, akin to legitimate e-commerce models (Decary-Hetu & Leppannen, 2013; Holt et al., 2015; Hutchings & Holt, 2015).

Once the final price is set, customers must then pay the vendor as no goods are tendered until payment is received. It may take days or weeks for vendors to deliver a customer's purchased goods in the case of drugs, firearms or other physical items (Copeland et al., 2020; Decary-Hetu et al., 2017; Moeller et al., 2017). Digital items, such as data, malicious software, or cybercrime services, can typically be accessed within minutes or hours of purchase depending (Franklin et al., 2007; Holt, 2012; Holt & Lampke, 2010). Regardless, there is a clear risk

that vendors may either simply fail to send the goods purchased, or provide adulterated or unusable items. For instance, stolen data vendors who fail to deliver customer products are referred to as “rippers” or rip off artists, and are viewed as a scourge on the market (Holt, 2012; Holt & Lampke, 2010; Hutchings & Holt, 2015). It is also possible that goods may be detected in transit and either seized or used to enable an arrest, as has been observed in the sale of both drugs and guns that are shipped through common package delivery services like DHL, UPS, and FedEx (Copeland et al., 2020; Decary-Hetu et al., 2016). In fact, a number of arrests have occurred in the US and UK because US Homeland Security investigators identify the weapons in transit and notify the appropriate law enforcement agencies at the destination residence (Copeland et al., 2020). Police then use the delivery as a cause to arrest individuals on charges related to the illegal purchase and possession of firearms.

In the event that products are not delivered or there is some problem with their quality, buyers must carefully review the terms of service for their purchase as they vary across vendors (Holt & Lee, 2020; Hutchings & Clayton, 2016; Hyslip & Holt, 2019). Typically, there are rules posted within each shop or advertisement within a forum or cryptomarket regarding what sellers support in terms of product replacements or errors in documents or delivered items. Many stolen data vendors offer free replacements for inactive cards within a 24 to 48-hour period of purchase, though some offer no such support (Holt & Lampke, 2010; Holt et al., 2015). Malware and cybercrime-as-service providers also operate customer support lines for customers in the event of product failure or error (Holt, 2013; Hutchings & Clayton, 2016). Some vendors for physical products, like drugs and stolen identity documents, clearly state that they do not offer refunds but may give conditional returns if the error is reported within a certain amount of time after purchase, or there was a clear error related to the purchased item (Dupont et al., 2016; Holt et al, 2016; Hutchings & Holt, 2015).

If the vendor adheres to posted policies, then the customer may be able to gain some satisfaction from the transaction. In the event they are ignored or unable to obtain the products they paid for, customers often have little recompense (Decary-Hetu et al., 2016; Moeller et al., 2017). A customer cannot contact police as they are essentially complicit in an illegal activity by virtue of their paying for drugs or cybercrime services. In addition, many vendors do not

accept payment via services that would allow the customer to dispute a charge (Decary-Hetu et al., 2016; Hutchings & Holt, 2017). As a consequence, participants in illicit markets have developed a number of different mechanisms that serve as informal sources of social control and risk avoidance strategies to minimize the likelihood of harm resulting from bad transactions.

One of the primary strategies employed over time has been the use of informal reviews of vendors in various markets. For instance, individuals who performed transactions with vendors who posted ads in forums were regularly able to post their experiences in the same thread (Decary-Hetu & Leppannen, 2013; Holt & Lampke, 2010; Holt et al., 2016). The direct feedback of the speed of communications and qualities of the seller gave potential customers an ability to discern who offered the best products at the most reasonable prices (Odabas et al., 2017; Smirnova & Holt, 2017). The presence of negative feedback served as a warning that the vendor may be unreliable, though positive and negative comments could be manufactured to influence the perception of their services (Odabas et al., 2017; Smirnova & Holt, 2017).

In recent years, third party reviewing services have emerged to provide insights on the qualities of vendors operating via shops and other platforms. For instance, the site Deep Dot Web served as an Open Web resource for individuals seeking information on vendors operating on the Dark Web (Department of Justice, 2021). The site provided information on the URLs of active shops and cryptomarkets, as well as informal news related to their operations and the quality of their services. The operators of the site were eventually arrested and prosecuted in the US on charges associated with money laundering (Department of Justice, 2021). Specifically, they were alleged to have received payments from individuals trafficking in drugs, guns, and other illicit products on the basis that they make positive comments about the vendors (Department of Justice, 2021).

An additional method of risk reduction that can be employed by market participants is the use of escrow payment systems (Decary-Hetu et al, 2016; Holt, 2012; Holt et al., 2015; Hutchings & Holt, 2015). The use of escrow in online markets mirrors that of traditional escrow services in legitimate business operations, wherein a third party holds funds as a guarantee of payment for a service provider. Escrow services were first observed in stolen data and malicious software sales in forums, where an individual within the forum's management

structure could be designated as an escrow provider on behalf of buyers and sellers (Decary-Hetu & Lepannen, 2013; Holt, 2012; Holt & Lampke, 2010). That individual could intervene in the sales process and hold funds from the customer with guaranteed deliver to the seller so long as the customer received products. Escrow operations typically came with a fee for their services, though they helped to create trust between participants as they could ensure both parties benefited from a transaction (Holt, 2012; Holt & Lampke, 2010).

Escrow services persist on both the Open and Dark Web, though they have become decentralized to some degree as forums have become less prevalent. Instead, escrow services now exist as independent operations and are an option for customers who are unsure of the reliability of a seller (Decary-Hetu et al., 2016; Moeller et al., 2017). If both parties accept the use of escrow, it can increase the likelihood of a successful transaction. At the same time, there is now risk related to the identification of a reliable escrow service provider who will not simply abscond with funds given by a potential customer. In fact, a number of cryptomarkets held payments in escrow on behalf of customers and buyers and simply shuttered their sites without completing any transactions. These events are colloquially referred to as exit scams, and have become a somewhat common occurrence in cryptomarket operations (Riley, 2019; Schwartz, 2020). It is unclear if exit scams occur as a long-term scheme on the part of scammers, or are a calculated decision by cryptomarket operators to close before police actions occur (Riley, 2019). Regardless, the presence of exit scams creates a risk that all participants must consider in their decision to engage in a transaction through Dark Web markets.

CHALLENGES AND DIRECTION FOR RESEARCH ON ILLICIT MARKET OPERATIONS

Though research on illicit markets in online spaces has grown dramatically over the last decade, there are still foundational questions that must be addressed. First, there is a need for continuous qualitative and quantitative explorations of the practices of the market to track shifts in both buyer and seller behaviors (Decary-Hetu et al., 2016; Dupont et al., 2017; Hutchings & Holt, 2017). This is particularly essential as the COVID19 pandemic has had a transformative impact on the supply chains for products, as well as the overall habits of consumers. The extent to which consumers may be interested in acquiring narcotics and pharmaceuticals for recreational or prescription needs must be better understood (Barratt & Aldridge, 2020; Bergeron et al., 2020; Groshkova et al., 2020). There is also a need for research addressing the extent to which COVID19 vaccines, vaccination cards, and related materials have flooded the market (Bergeron et al., 2020; Groshkova et al., 2020).

Additionally, foundational research considering the decision-making processes of buyers for various products must be performed. For instance, several studies noted the rise of firearms markets on the Dark Web, though it is unclear who vendors are targeting with their advertisements (Copeland et al., 2020; Paoli et al., 2017). Survey research attempting to identify how many individuals in countries with restrictive gun laws have sought out weapons online may help to improve our understanding of the general audience for these ads (Copeland et al., 2020). Similar studies have explored the purchasing habits of narcotics users in Australia (Barratt et al., 2017), suggesting it may be possible to perform similar work regarding other illicit products, including identity documents (Holt & Lee, 2020) and firearms (Copeland et al., 2020).

The same is true regarding the ways that potential buyers identify vendors for products in the increasingly fragmented advertising environment for illicit goods. Not only do vendors operate on shops, forums, and cryptomarkets, but have also begun to sell products on social media platforms and communications systems (Bachhuber & Merchant, 2017; Moyle et al., 2019). This adds to the inherent difficulty in identifying vendors and distinguishing their legitimacy (Tzanetakis et

al., 2017). Qualitative investigations of customers would be essential to better understand the ways that they negotiate the online market and authenticate vendor claims over time (Holt et al., 2015; Hutchings & Holt, 2017).

Research is also needed to better understand the decision-making processes of vendors who operate illicit markets. Though there has been substantive focus on the perceived and real legitimacy of vendors operating in various markets (e.g Decary-Hetu & Leppanen, 2013; Holt et al., 2016), few have considered the factors that drive individuals to post advertisements for goods that are likely false. For instance, research and media reporting have noted the range of hitman advertisements on the Dark Web (Kassab & Rosen, 2019; Roddy & Holt, 2020). These sites are thought to be false, and serve only to rip off potential customers (Kassab & Rosen, 2019; Roddy & Holt, 2020). It is assumed that such ads generate profits for advertisers, though it is unclear if any other thought processes guide the decision to make false ads (Roddy & Holt, 2020). Additionally, it is unclear if such vendors operate multiple fictitious ads, or operate in both legitimate and fraudulent products simultaneously. Such work is vital to improve our knowledge of the extent to which fraud is a specific or general characteristic of illicit market operations in online spaces.

Similarly, work is needed to assess what factors compel vendors to engage in activities on the Open or Dark Web, or both environments simultaneously. For instance, a small number of studies has observed differences in both the quantities, qualities, and prices for products for sale when comparing Open and Dark Web advertisements (Holt & Lee, 2020; Smirnova & Holt, 2017). It is thought that such differences may be a function of the global reach of vendors on the Open Web relative to the Dark Web, which has a small, Western-nation user base (Holt & Lee, 2020; Smirnova & Holt, 2017). Research is needed to assess whether such differences stem from deliberate decision-making on the part of vendors to operate differently across environments. Furthermore, the degree to which vendors decide where to advertise on the basis of perceived risk of detection or other factors, such as an inability to be extradited or prosecuted must be explored (Decary-Hetu et al., 2017; Hutchings & Holt, 2017). Such research could greatly expand our knowledge of the degree to which rational choice and deterrent efforts guide the behaviors of vendors.

In much the same way, empirical inquiry is needed to understand the ways

that illicit markets for products persist in the face of law enforcement crackdowns (Decary-Hetu et al., 2016; Holt, Blevins, & Kuhns, 2008; 2014). For instance, a series of arrests were made by police agencies in the US and Europe, targeting both the customers and operators of booter and streser services (Jeffrey, 2018; Krebs, 2018; Krebs, 2019). Recent analyses suggest that the number of attacks performed by service providers decreased in the wake of enforcement efforts (Collier et al., 2019: Pritchard, 2020). Though these investigations reduced the operational capacities of vendors, the risk of arrest and detection was not enough to eliminate their operations from the Internet (Collier et al., 2019). Thus, research is needed to consider why and how these offenders practice restrictive deterrence strategies to continue offending (Collier et al., 2019; Holt & Bossler, 2016; Holt et al., 2015).

Finally, there is a need for researchers to identify data sources that extend beyond the current sampling strategies used in published studies (Holt & Dupont, 2019; Holt & Bossler, 2015; Yip et al., 2013). Most academic data is derived from shops, forums, and cryptomarkets that can be accessed by the general public. Though useful, this data only informs our understanding of the surface level, open markets that exist (Decary-Hetu et al., 2016; Holt & Dupont, 2017; Hutchings & Holt, 2017). The practices of those actors engaged in more serious, closed markets are less frequently examined due to the inherent difficulty in accessing these sources. Closed communities can require payment or social vetting in order to gain entry, which limits the ability of researchers to engage due to the ethical constraints in place in university settings (e.g. Holt & Bossler, 2015; Yip et al., 2013).

As a consequence, there is a need for researchers to develop alternative strategies for data collection that would improve our understanding of closed communities. For example, hacked or leaked data from forums have been used by researchers to understand the practices of hacker communities (Dupont et al., 2017; Holt & Dupont, 2019). Such data presents its own unique ethical dilemmas for researchers as the data may have been acquired illegally, even if it is available for public download (Holt & Bossler, 2015). Instead, researchers may find value in developing surveys and interview protocols that could be administered to active participants within these communities (e.g. Barratt et al., 2017; Hutchings & Holt, 2017). While they present a high risk of failure due to

low response rates, they could produce valuable findings in ways that conform to existing ethical guidelines.

Additionally, developing data through police files could be informative to understand the practices of known criminals and their associates (Holt & Bossler, 2015; Leukfeldt et al., 2017). Such efforts require collaborative agreements with law enforcement and cybersecurity providers could also prove invaluable as they have the capacity to access these communities. Creating memorandums of understanding that would enable data sharing without attribution to ongoing investigations or tradecraft could be extremely useful to understand the ways actors engage with one another without violating ethical practices (Holt & Bossler, 2015; Hutchings & Holt, 2017).

CONCLUSION

Criminological scholarship on illicit markets operating in online spaces has grown dramatically over the last two decades, assessing the state of both physical and digital goods for sale (Decary-Hetu et al., 2017; Holt & Bossler, 2015; Hutchings & Holt, 2017). The growth of the Internet, e-commerce applications, encrypted communications platforms and financial services have created an operating environment where virtually any good or service can be sold, mirroring the activities of real world illicit goods markets. These studies demonstrate the similarities between the practices of vendors and buyers operating in virtual and real spaces, particularly regarding the process of navigating illicit transactions (Barratt, 2012; Holt & Dupont, 2019; Holt et al., 2015; Hutchings & Holt, 2017). There are distinctions, however, in the risks that they face from law enforcement and from informal threats such as fraudulent vendors (Decary-Hetu et al., 2017; Holt et al., 2016; Tzanetakis et al., 2016).

Research on the processes of markets on both the Open and Dark Web provide substantive insights into the ways these forms of cybercrime are driven by social forces and assessments of risk and reward. These studies highlight potential opportunities for law enforcement, ISPs, and other place managers to more effectively regulate online spaces and limit the scope of illicit market operations (Hutchings & Holt, 2017). At the same time, the evolution of technology and its acceptance by the public will undoubtedly force changes in the practices of illicit markets in both virtual and real settings. The rise of cryptomarkets and various digital currencies will likely be replaced by other platforms in the near future, due in part to their perceived ease of use and minimized risk of detection by law enforcement (Holt et al., 2016). For instance, the use of encrypted messaging applications and social media may have a transformative impact on both virtual and real markets for illicit narcotics (Bachhuber & Merchant, 2017; Moyle et al., 2019). Thus, researchers must be vigilant in their investigation of illicit economies, regardless of where they operate to better understand their social and financial processes and ensure the efficacy of criminal justice responses to these offenses.

References

Adler, P. A. (1993). *Wheeling and dealing: An ethnography of an upper-level drug dealing and smuggling community*. Columbia University Press.

Bachhuber, M. A., & Merchant, R. M. (2017). Buying drugs online in the age of social media. *American journal of public health*, *107*(12), 1858.

Barratt, M. J. (2012). Silk Road: eBay for drugs. *Addiction, 107*/3: 683-683.

Barratt, M. J., & Aldridge, J. (2020). No magic pocket: Buying and selling on drug cryptomarkets in response to the COVID-19 pandemic and social restrictions. *International Journal of Drug Policy*, *83*, 102894.

Barratt, M. J., Ferris, J. A., Zahnow, R., Palamar, J. J., Maier, L. J., & Winstock, A. R. (2017). Moving on from representativeness: testing the utility of the Global Drug Survey. *Substance Abuse: Research and Treatment*, *11*.

Bateman, S. (2021). Sex slaves, human hunting trips, hitmen for hire: Dark web expert sorts fact from fiction. Daily Star, January 3, 2021. https://www.dailystar.co.uk/news/weird-news/sex-slaves-human-hunting-trips-23097531

Bergeron, A., Décary-Hétu, D., & Giommoni, L. (2020). Preliminary findings of the impact of COVID-19 on drugs crypto markets. *International Journal of Drug Policy*, *83*, 102870.

Carr, A. (2011). The Craigslist Crime Report: "Cesspool of Crime," Bold Use of Marketing. Fast Company, Feb. 24, 2011. https://www.fastcompany.com/1731352/craigslist-crime-report-cesspool-crime-bold-use-marketing-updated

Cook, P. J., Cukier, W., & Krause, K. (2009). The illicit firearms trade in North America. *Criminology & Criminal Justice*, *9*(3), 265-286.

Cooper, J., & Harrison, D. M. (2001). The social organization of audio piracy on the Internet. *Media, Culture & Society*, *23*(1), 71-89.

Copeland, C., Wallin, M., & Holt, T. J. (2020). Assessing the practices and products of Darkweb Firearm vendors. *Deviant Behavior*, *41*(8), 949-968.

Cunningham, S., & Shah, M. (eds., 2016). *The Oxford Handbook of the Economics of Prostitution.* Oxford: Oxford University Press.

Décary-Hétu, D., & Giommoni, L. (2017). Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous. *Crime, Law and Social Change*, *67*(1), 55-75.

Décary-Hétu, D., Paquet-Clouston, M., & Aldridge, J. (2016). Going international? Risk taking by cryptomarket drug vendors. *International Journal of Drug Policy*, *35*, 69-76.

Décary-Hétu, D., & Leppänen, A. (2013). Criminals and signals: An assessment

of criminal performance in the carding underworld. *Security Journal*, 31: 1-19.

Department of Justice (2021). DeepDotWeb administrator pleads guilty to money laundering conspiracy. March 31, 2021. Washington D.C. [Online] Available at: https://www.justice.gov/opa/pr/deepdotweb-administrator-pleads-guilty-money-laundering-conspiracy

Dupont, B., Côté, A.-M. Boutin, J.-I., & Fernandez, J. (2017). Darkode: Recruitment patterns and transactional features of "the most dangerous cybercrime forum in the world." *American Behavioral Scientist* 61: 1219-1243.

Eck, J. (1995). A General Model of the Geography of Illicit Retail Marketplaces, in J. Eck and D. Weisburd, eds., *Crime and Place.Crime Prevention Studies, Vol.4.* Monsey, New York: Criminal Justice Press

Gibbs, J. (1975). *Crime, Punishment, and Deterrence*. New York: Elsevier.

Groshkova, T., Stoian, T., Cunningham, A., Griffiths, P., Singleton, N., & Sedefov, R. (2020). Will the current COVID-19 pandemic impact on long-term cannabis buying practices?. *Journal of Addiction Medicine*.

Hamid, A. (1998). *Drugs in America.* Gaithersburg, MD: Aspen

Holt, T. J. (2010). Exploring strategies for qualitative criminological and criminal justice inquiry using online data. *Journal of Criminal Justice Education, 21*/4: 466-487.

Holt, T. J. (2013). Examining the forces shaping cybercrime markets online. *Social Science Computer Review, 31*/2: 165-177.

Holt, T. J., & Bossler, A. M. (2015). *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. London: Routledge.

Holt, T. J., Blevins, K. R., & Kuhns, J. B. (2014). Examining diffusion and arrest practices among johns. *Crime and Delinquency,* 60, 261–283.

Holt, T. J., & Dupont, B. (2019). Exploring the factors associated with rejection from a closed cybercrime community. *International journal of offender therapy and comparative criminology*, *63*(8), 1127-1147.

Holt, T. J. & Lampke, E. (2010). Exploring stolen data markets online: Products and market forces. *Criminal Justice Studies, 23*/1: 33-50.

Holt, T. J., & Lee, J. R. (2020). A Crime Script Analysis of Counterfeit Identity Document Procurement Online. *Deviant Behavior*, 1-18.

Holt, T. J., Smirnova, O., & Chua, Y. T. (2016). *Data thieves in action: Examining the international market for stolen personal information.* New York: Palgrave.

Holt, T. J., Smirnova, O., Chua, Y. T., & Copes, H. (2015). Examining the risk reduction strategies of actors in online criminal markets. *Global Crime*, *16*(2), 81-103.

Holt, T. J., Smirnova, O., & Hutchings, A. (2016). Examining signals of trust in criminal markets online. *Journal of Cybersecurity*, *2*(2), 137-145.

Hospodar, M. (2021). 10 Underrated Horror Games (That Came Out in the Last 5 Years). Gamerant, Febuary 11, 2021. https://gamerant.com/underrated-horror-games-last-5-years/

Hureau, D. M., & Braga, A. A. (2018). The trade in tools: The market for illicit guns in high-risk networks. *Criminology*, *56*(3), 510-545.

Hutchings, A., & Clayton, R. (2016). Exploring the provision of online booter services. *Deviant Behavior*, *37*(10), 1163-1178.

Hutchings, A., & Holt, T. J. (2015). A crime script analysis of the online stolen data market. *British Journal of Criminology, 55*/3*:* 596-614.

Hutchings, A., & Holt, T. J. (2017). The online stolen data market: disruption and intervention approaches. *Global Crime*, *18*(1), 11-30.

Jacobs, B. A. (1996). Crack dealers' apprehension avoidance techniques: A case of restrictive deterrence. *Justice Quarterly, 13*/3: 359-381.

Jacobs, B. A. (2000). *Robbing drug dealers: Violence beyond the law.* Boston: Northeastern University Press.

Jacobs, B. A. (2010). Deterrence and Deterrability. *Criminology* 48: 417-441.

Johnson, B. D., & Natarajan, M. (1995). Strategies to avoid arrest: Crack sellers' response to intensified policing. *American Journal of Police, 14*/3/4: 49-69.

Johnson, B. D., Dunlap, E., & Tourigny, S. C. (2000). Crack distribution and abuse in New York. *Crime prevention studies*, *11*, 19-58.

Kassab, H. S., & Rosen, J. D. (2019). Illicit Markets and the Internet Age. In *Illicit Markets, Organized Crime, and Global Security* (pp. 155-175). Palgrave Macmillan, Cham.

Kennedy, D. M., Piehl, A. M., & Braga, A. A. (1996). Youth violence in Boston: Gun markets, serious youth offenders, and a use-reduction strategy. *Law and Contemporary Problems*, *59*(1), 147-196.

Klokars, C. B. (1974). The Professional Fence. New York: The Free Press.

Knowles, G. J. (1999). Deception, detection, and evasion: A trade craft analysis of Honolulu, Hawaii's street crack-cocaine traffickers. *Journal of Criminal Justice*, *27*(5), 443-455.

Lavorgna, A. (2014). Wildlife trafficking in the Internet age. *Crime Science*, *3*(1), 1-12.

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

May, T., & Hough, M. (2004). Drug markets and distribution systems. *Addiction Research and Theory*, 12: 549-563.

Meyer, G. R. (1989). *The Social Organization of the Computer Underground.*

Master's thesis, Northern Illinois University.

Moeller, K., Munksgaard, R., & Demant, J. (2017). Flow my FE the vendor said: Exploring violent and fraudulent resource exchanges on cryptomarkets for illicit drugs. *American Behavioral Scientist*, *61*(11), 1427-1450.

Moyle, L., Childs, A., Coomber, R., & Barratt, M. J. (2019). # Drugsforsale: An exploration of the use of social media and encrypted messaging apps to supply and access drugs. *International Journal of Drug Policy*, *63*, 101-110.

Paoli, G. P., Aldridge, J., Nathan, R., & Warnes, R. (2017). *Behind the curtain: The illicit trade of firearms, explosives and ammunition on the dark web.* Santa Monica, CA: Rand: [Online] Available at: https://www.research.manchester.ac.uk/portal/files/57841517/RAND_Behind_the_curtain.pdf

Potter, G. (2009). Exploring retail-level drug distribution: Social supply,"real" dealers and the user/dealer interface. *Old and new policies, theories, research methods and drug users across Europe*, 50-74.

Power, M. (2013). Online highs are as old as the net: The first e-commerce was a drugs deal. The Guardian, April 19, 2013. https://www.theguardian.com/science/2013/apr/19/online-high-net-drugs-deal

Riley, D. (2019). $30M stolen as popular dark web market closes. siliconANGLE, April 23, 2019. https://siliconangle.com/2019/04/23/30m-stolen-popular-dark-web-market-pulls-exit-scam/

Roddy, A. L., & Holt, T. J. (2020). An Assessment of Hitmen and Contracted Violence Providers Operating Online. *Deviant Behavior*, 1-13.

Schneider, J. L. (2005). Stolen-Goods Markets: Methods of Disposal 1. *British Journal of Criminology*, *45*(2), 129-140.

Schwartz, M. J. (2020). Bye-bye Bitcoins: Empire Darknet Market 'Exit Scams'. Euro Security Watch, September 2, 2020. https://www.bankinfosecurity.com/blogs/bye-bye-bitcoins-empire-darknet-market-exit-scams-p-2934

Scott, M. S., & Dedel, K. Street prostitution. *Problem Oriented Policing Guide Series (2)*. Washington D.C.: Office of Community Oriented Policing Services, U.S. Department of Justice.

Smirnova, O., & Holt, T. J. (2017). Examining the geographic distribution of victim nations in stolen data markets. *American Behavioral Scientist*, *61*(11), 1403-1426.

Sollund, R. A. (2019). *The crimes of wildlife trafficking: Issues of justice, legality and morality*. London: Routledge.

Sterk, C. (1999). *Fast lives: Women who use crack cocaine.* Philadelphia, PA: Temple University Press.

Topalli, V., Wright, R., & Fornango, R. (2002). Drug dealers, robbery and retaliation. Vulnerability, deterrence and the contagion of violence. *British Journal of Criminology, 4*2/2: 337-351.

Turnbull, R. (2002). *A Rock and a Hard Place: Drug Markets in Deprived Neighbourhoods*. Home Office Research Study No. 240. London: Home Office.

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*, 35: 58-68.

VanNostrand, L. M., & Tewksbury, R. (1999). The Motives and Mechanics of Operating an Illegal Drug Enterprise." *Deviant Behavior* 20/1: 57-83.

Weitzer, R. (2012). *Legalizing prostitution: From illicit vice to lawful business*. NYU Press.

Wright, R., & Decker, S. H. (1994). *Burglars On the Job: Streetlife and Residential Break-ins.* Boston, MA: Northeastern University Press.

Wright, R., & Decker, S. H. (1997). *Armed Robbers in Action: Stickups and Street Culture.*

Boston, MA: Northeastern University Press.