Contextualizing Online Illicit Market Economies

Ariel L. Roddy and Jin R. Lee, School of Criminal Justice, Michigan State University
roddyari@msu.edu, leejin26@msu.edu

ABSTRACT: While the Internet has many benefits, its growth has contributed to the emergence of online illicit markets through the Open and Dark Web. It is possible to envision these markets as an economy of both material goods and an economy of knowledge, ideas, and information, which can be used to facilitate criminal behavior. This brief provides an overview of online markets operating on Open and Dark Web sites, focusing on how individuals can come to these markets to both buy and sell products, and engage in offending writ large.

The value of the Internet cannot be understanding for information sharing and knowledge dissemination. At the same time, it has become a platform for online illicit markets running through the Open and Dark Web. While much has been written about the Open Web market activities occurring, there has been less focus on those operating through sites hosted on the Dark Web. The relatively recent emergence of content hosted through Tor and I2P, the so-called Dark Web, is thought to be invaluable to offenders because its encryption tools conceal the real-world identity and location of participants and servers generally.[1]

The economic exchanges occurring across illicit online markets can straddle the bounds of online and offline crime. Individuals offer virtual storefronts for illicit products and services that can be consumed in the real-world.[2] These sites also create a knowledge economy, whereby individuals share information that can be used to engage in criminal activity. Such exchanges can take different forms, ranging from unsolicited advice shared in text, video, and audio-based tutorials to direct engagement via forums and other communications media.[3] We will explore each form of exchange and the ways they facilitate economic or knowledge transfers.

Material Economies on the Web

Cybercriminals can congregate in online settings to engage in business transactions where a wide variety of products and services are exchanged. The bulk of products sold through illicit online markets generally consist of *stolen data* (e.g., credit cards, login IDs and passwords, bank accounts, online payment accounts, and other personal identifying information); *cybercrime tools* (e.g., malware, hacking tools/packages, botnets, and phishing kits); *services* (e.g., cash out services and consulting); *illegal drugs*; and *firearms*.[4] [5]

Participants within these markets vary in terms of technical skill and expertise.[6] Vendors, such as those offering money mule services or stolen data, may not have great technical skill, but are instead focused on garnering profits from the sale of goods and services.[7] Individuals offering malware and tools may, however, have greater skill due to the sophistication needed to produce or maintain their products over time. In addition, some vendors with greater computer skills may serve additional roles as market moderators and content experts.[8]

Forum-based markets will be managed or maintained by moderators, who can increase trust among participants and ensure safer transactions by strictly enforcing community rules for participation.[9] Sellers and buyers may also adopt additional modes of communication

[1] Martin, 2014
[2] Barratt & Aldridge, 2016
[3] Hutchings, 2014
[4] Albon, 2018
[5] Leukfeldt, Kleemans, & Stol, 2017
[6] Albon, 2018
[7] Albon, 2018
[8] Albon, 2018
[9] Holt, Smirnova, & Hutchings, 2016

to enhance privacy and security, such as private messaging systems within the forum or encrypted email exchanges outside the forum on the Dark Web.

Buyers, regardless of whether the transaction is completed via a forum or single-operator shop, are often encouraged to leave positive or negative feedback about their experience.[10] The post should provide information on the buyer's encounter, including the quality of the goods or service, the delivery time, and the speed of communication with the vendor. The information provided in feedback creates an informal social force to manage participant behavior to maximize rewards and reduce risk for buyers and sellers[11].

Information Economies on the Web

Beyond purchasing physical goods or technical services, the Internet has enabled the formation of information economies, defined broadly as "a group of establishments, firms, institutions, organizations, and departments, or teams within them...that produce knowledge, information services or information goods, either for their own use or for use by others"[12]. These economies often resemble online forums, message boards, or Internet-Relay-Chat (IRC) communities.

Some of these mediums facilitate the exchange of information regarding successful completion of offline crimes, including soliciting sex work, purchasing illegal drugs, and building or obtaining illegal weapons.[13] The nuances of these criminal practices are discussed, including pricing and procedural practices, as well as advice on avoiding scams and law enforcement detection.[14]

Other forums, message boards, and IRC offer a space for discussion and instruction related to online crimes. Individuals on message boards can post hacking tutorials, pieces of computer code, and links to other online resources to assist in hacking or other cyber-attacks[15]. Given the highly visible nature of forums, and the anonymity and protection provided by the Dark Web, users are able to share this information to a wide audience with impunity. Forums, message boards, and IRCs also function as a way for cybercriminals to build co-offending networks and remotely launch cyberattacks.[16]

Conclusion and Implications

The advent of the Internet has significantly altered the landscape of crime, both on and offline. It offers material economies, in which individuals can solicit real-world goods and services, though there are also offender information sharing networks that brazenly operate in the open in which criminal behavior is outlined in great detail.

As a result, it is feasible for an individual with little cybercrime understanding to gain knowledge of offending by visiting a forum on the Open or Dark Web and consuming its contents. These communities dramatically increase access to illicit products, improve the knowledge capital of online criminals, and facilitate the creation of co-offending networks. It is imperative that researchers and law enforcement alike improve our understanding of the processes of these communities and find ways to disrupt their operations in order to limit their role in offending generally.

References

Ablon, L. (2018). The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data.

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.

[10] Holt, Smirnova, Chua, & Copes, 2015
[11] Holt & Lampke, 2010
[12] Machlup, 1980
[13] Gehl, 2014
[14] Blevins & Holt, 2009
[15] Benjamin & Chen, 2014
[16] Benjamin & Chen, 2014

Benjamin, V., & Chen, H. (2014). Time-to-Event Modeling for Predicting Hacker IRC Community Participant Trajectory. In *2014 IEEE Joint Intelligence and Security Informatics Conference* (pp. 25–32).

Blevins, K. R., & Holt, T. J. (2009). Examining the Virtual Subculture of Johns. *Journal of Contemporary Ethnography, 38*, 619–648.

Gehl, R. W. (2016). Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network. *New Media & Society, 18*, 1219–1235.

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

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

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.

Hutchings, A. (2014). Crime from the keyboard: organised cybercrime, co-offending, initiation and knowledge transmission. Crime, *Law and Social Change*, 62, 1–20.

Leukfeldt, R., Kleemans, E., & Stol, W. (2017). The Use of Online Crime Markets by Cybercriminal Networks: A View From Within. *American Behavioral Scientist*, *61*(11), 1387–1402.

Martin, J. (2014). *Drugs on the dark net: how cryptomarkets are transforming the global trade in illicit drugs*. Houndmills, Basingstoke, Hampshire; New York, NY: Palgrave Macmillan.