Digital Drug Lords

Lilly Sharples

March 19, 2021

In today's technologically driven world, it is no surprise that even criminals are moving their work to the internet. Cybercrime, "any and all illegal activities carried out using technology"[1], allows both individuals and global groups to commit crimes on a larger scale. With technology constantly developing, it is no surprise that cybercrime is the fastest growing area of criminal activity. The possibilities with online crime are unimaginable. In fact, it is estimated that "cybercrime will cost the planet $6 trillion in damages by 2021"[2]. Moving criminal activity online allows for anonymity between individuals and governing bodies through encryption, as well as easy illicit payments through cryptocurrency. One major way online crime is seen is through drug deals.

When addressing digital drug deals, cybercrimes can be executed on the surface web, social media platforms, and the deep/dark web. The surface web is everything public. With an example of a google search, the list of pages returned as a result are part of a connected database. Through this database, users can be led to other relevant pages based on their search history. Websites, blogs, and even comments on the surface web can all be traced back to their source, with very little privacy unless other measures are taken(VPN, encryption software, etc.). This lack of privacy means fewer crimes are seen on the surface web, however those experienced with technology can find ways around this. There are still an abundance of crimes committed on the surface web every day, such as "identity theft, hacking…sports betting, fraud, spying, piracy or theft(illegal downloading), developing and selling malware(viruses, worms, etc.), purchasing illegal materials, and stolen property"[3].

[1] Nica Latto. What is Cybercrime and How Can You Prevent It? Avast, December 19, 2020. https://www.avast.com/c-cybercrime#topic-6.
[2] Hanna Samir Kassab and Jonathan D. Rosen. 2019. Illicit Markets, Organized Crime, and Global Security. Palgrave Macmillan imprint published by Springer International Publishing AG.
[3]Kassab, 158

With the worldwide adoption of social media over the last decade, it is no surprise that criminal activity has found its place on various online platforms. Much like the surface web, social media still lacks anonymity, and therefore comes with a risk of being caught. Private accounts, groups, and posts are not as private as you may think, and require advanced technology to eliminate the ability to be traced to the origin. One common way social media is being used for illicit drug trades is through Facebook groups. These groups require permission to enter, and have moderators who confirm or deny users. Drug dealers can create burner accounts, using fake names and profiles, and post in these groups. This allows dealers to connect with individuals in their area without immediately showing their identity. Most of the time, "people selling drugs on social media are not hidden behind encryption...and they physically meet with the buyers to exchange goods and money"[4]. Having to meet up for these exchanges still poses risk of violence or getting caught, making social media a lesser used platform for digital drug deals.

The dark or deep web is most widely known for illegal activity. This is the hidden part of the web, requiring specific software and technical knowledge to reach specific content/web pages. Dark web searches are hidden from surface web browsers, and are unconnected-unlike a google search, where everything is linked in a publicly connected database. Though the dark web is a broad term, dynamic web pages, blocked sites, unlinked/private sites, content encoded in a different format inaccessible by normal web searches, and limited access networks'[5] are examples of what is accessed. In order to access this secret content, three main anonymous networks are used.

[4] Silje Anderdal Bakken, "Drug Dealers Gone Digital: Using Signalling Theory to Analyse Criminal Online Personas and Trust," Global Crime, August 20, 2020, https://www.tandfonline.com/doi/citedby/10.1080/17440572.2020.1806826?scroll=top&needAccess=true.

[5] Vincenzo Ciancaglini, Marco Balduzzi, and Robert McArdle, "Deep Web and Cybercrime: It's Not All About Tor," Deep Web and Cybercrime: It's Not All About Tor - Wiadomości bezpieczeństwa, November 12, 2014, https://www.trendmicro.com/vinfo/pl/security/news/cybercrime-and-digital-threats/deep-web-and-cybercrime-its-not-all-about-tor, 3.

The Onion Router, more commonly referred to as TOR, is the most popular encrypted routing software. This means that "messages are encapsulated in layers of encryption"[6]. Data starts at the first/origin node, and each consequent node peels away/decrypts a layer, sending the data to the next node. At the final layer, the data arrives at its location. Since each node only knows the node before and after it, the origin and final destination are untraceable. The entire network uses over three thousand nodes, with multiple layers to ensure anonymity. TOR was originally developed by the U.S Naval Research Laboratory in 2002, to encrypt and protect online government communication[7]. Now, entire sites can be untraceably hosted on TOR nodes, with client and server IP addresses remaining hidden.

Freenet is another network also developed in 2002. It is less popular than TOR, due to being "more suitable to serving static content such as static sites and does not cope well with dynamically generated web pages or other forms of Internet services (e.g., IRC, mail, etc)"[8]. Simple marketplaces are still seen through Freenet, where malicious transactions take place daily. Invisible Internet Project was designed in 2003 as an anonymous peer-to-peer distributed communication layer. Also known as I2P, the primary use is encrypted communication by means of file sharing between users. It is a decentralized network database, but is said to be "more resilient to infiltration or monitoring"[9] than TOR.

It is one thing to have your identity hidden through encryption when making sales/purchases via online drug markets. The next important factor is cryptocurrency, an untraceable and decentralized form of payment. Since Bitcoin's creation in 2009, the cryptocurrency has gained a reputation for illegal payments. Similar to the encryption techniques

[6] Hanna Samir Kassab and Jonathan D. Rosen. 2019. Illicit Markets, Organized Crime, and Global Security, 159.

[7] Vincenzo Ciancaglini, Marco Balduzzi, and Robert McArdle, "Deep Web and Cybercrime: It's Not All About Tor", 5.

[8] Vincenzo Ciancaglini, 7.

[9] Hanna Samir Kassab and Jonathan D. Rosen. 2019. Illicit Markets, Organized Crime, and Global Security, 160.

used in anonymous networks, using special hash code on the blockchain allows for fast and secure transactions. As Bitcoin is universal and decentralized, there is no need for expensive and time consuming currency exchanges. A universal currency is especially important within digital drug markets, where most illicit drugs are grown/produced in different countries than their final destination.

Cryptomarkets, which may also be referred to as darknet markets, are digital marketplaces where anonymous vendors can sell illegal items. Successful cryptomarkets contain Bitcoin, Tor and PGP encryption as central components[10]. This is not saying that other servers, cryptocurrencies, or encryption methods do not work, but the last ten years have seen success with the aforementioned. For example, the original Silk Road marketplace built on TOR was extremely popular from its creation in 2011 until it was shut down in 2013. Silk Road Reloaded was an attempted black market run on the I2P network, but did not gain as much popularity as competing popular markets run through TOR. In terms of drug markets, "there is a tendency for the economy to centralize on a few marketplaces"[11]. The centralization of markets is likely due to the dangerous nature of drugs. Markets with an abundance of strong reviews will attract customers, while they will steer clear of markets with negative reviews for their safety. This is seen within the popular Agora marketplace, which had 238,914 reviews in the cannabis category, making consumers feel safer that others had used the products they were purchasing.

It is important to discuss the target market of online drug sales. These marketplaces require technological skills more advanced than the average person, meaning cryptomarkets cater to those buyers who intend to buy large amounts of product and redistribute locally. For example,

[10] Jakob Demant, Rasmus Munksgaard and Esben Houborg. Personal use, social supply or redistribution? cryptomarket demand on Silk Road 2 and Agora. *Trends Organ Crim* 21, 42–61 (2018). https://doi.org/10.1007/s12117-016-9281-4.

[11] Jakob Demant

"the largest purchases observed were two custom orders on Agora at 87,256 USD each"[12]. Online drug marketplaces may be the beginning of smaller, local drug dealing networks. This results in a structure where digital vendors become digital drug lords, controlling a network of drug dealers they may never know the name of.

When comparing traditional street drug sales and online drug sales, the benefits of cryptomarkets are clear. Drug deals are less risky and violent for both parties, as everyone remains anonymous and there is no space for physical violence. Funds are instantly transferred to the seller via cryptocurrency, and the illicit packages are inconspicuously shipped alongside normal mail. There is a more formal aspect when selling drugs online, such as "advertising and customer service in the form of correct grammar, photographs of the drugs for sale, reputation and stealth"[13]. Similar to any legal business, popular cryptomarkets want to keep their reputation in order to maximize profit.

With the sole idea of cryptomarkets being anonymous, it is hard for governments to shut these marketplaces down and hold the founder(s) responsible. The original Silk Road cryptomarket was shut down in October of 2013 by the DEA and FBI, after two years of unstoppable illicit sales. Less than a month later, Silk Road 2 was created, along with other marketplaces[14]. With stronger encryption techniques being developed, it is becoming increasingly difficult to find, access, and shut down these markets. It is not as easy as finding drug offenders on the street and arresting them.

Another challenge of shutting down drug markets deals with jurisdiction. The seller and consumer are more than likely in different locations across the world. An emerging idea is that

[12] Jakob Demant

[13] Jakob Demant, Rasmus Munksgaard and Esben Houborg. Personal use, social supply or redistribution? cryptomarket demand on Silk Road 2 and Agora.

[14] Jakob Demant

"cyberspace should be designated a separate and unique jurisdiction"[15]. Therefore, crimes committed through the dark web will be processed in a different way than normal criminal activity.

Other than the obvious broken law of illegal drug sales, there is the factor of unlawful use of technology, as well as other crimes commited to accomplish this. For example, the founder of Silk Road, was "sentenced to life without parole for drug trafficking, fraudulent identity tracking, hacking crimes, and money laundering"[16]. Using encryption for illegal use is the base of cryptomarkets, so it is assumed that market founders will be prosecuted for this as well. In order to decrypt, shut down, and correctly prosecute these criminals, cybersecurity teams will be increasingly beneficial in the legal field. Right now, the average lawyer does not understand the advanced technological skills related to encryption, and "our laws are not current enough to adequately address all the possible forms of cybercrime"[17]. It is therefore necessary for the future of law to evolve alongside continued technological advancement. A new generation of lawmakers with technological knowledge is necessary to tackle the new era of cybercrime and digital drug lords.

[15] Donald R Dixon. 2019. "Cybercrime Investigation." Salem Press Encyclopedia.

[16] Hanna Samir Kassab and Jonathan D. Rosen. 2019. Illicit Markets, Organized Crime, and Global Security, 163.

[17] Nica Latto. What is Cybercrime and How Can You Prevent It?