CIVITAS, 2025, 15(1), 285-309
www.civitas.rs

Petrović Ivica[1]
Kovačević Igor[2]

UDC 004.738.5:343.9.024
Preliminary Communication
Received: 26/03/2024
Accepted: 15/09/2024

INTERNET AS ILLICIT DRUG MARKET

Abstract: Over the past decade, technological advancements driven by digitalization have transformed everyday life, enhancing communication, expanding access to information and education, and reshaping business operations. However, these developments have also facilitated new forms of criminal activity, particularly drug trafficking through hidden online networks. This paper examines the complex dynamics of online drug markets, analyzing DarkNet's role in shaping the operations of both organized crime groups and individual traffickers. It highlights major cryptomarkets such as Silk Road and Hydra, which operated clandestinely for years as platforms for the sale of illicit drugs and other illegal goods and services.

Keywords: DarkNet, online drug trafficking, cryptomarkets, dead drop, Covid-19.

1. Introduction

In the era of digital transformation, technological advancements have not only streamlined daily life but have also created new avenues for criminal activity. One of the most pressing challenges emerging from this shift is the rise of online drug trafficking. While traditional drug distribution methods remain relevant, the digital landscape has become

[1] Professor at the National Security Academy, Assoc. Prof. E-mail: prokupac3@gmail.com

[2] Master of Science in Electrical Engineering, Security Information Agency, email: kovacig@gmail.com

a critical hub for illicit trade, offering criminals anonymity, global reach, and sophisticated techniques to evade law enforcement.

This paper examines the complex dynamics of online drug trafficking, investigating how digital platforms serve as conduits for both organized crime syndicates and independent traffickers. By analyzing technological, legal, and socio-economic factors, it seeks to provide a comprehensive understanding of the multifaceted nature of this issue, assess current countermeasures, and explore the broader implications of cyber-enabled drug markets on society and global security.

2. Online drug trafficking

Since 2011 and the establishment of the first crypto drug market "Silk Road", "the number of anonymous online drug markets has expanded and online commerce has become a common way to buy and sell illegal drugs" (United Nations Office on Drugs and Crime, 2021). A large number of studies have "dealt with drug trafficking through the DarkNet" (Aldridge, Stevens & Barratt, 2018), including "coordination between buyers and sellers" (Bakken, Moeller & Sandberg, 2018) and methods aimed at creating and maintaining trust between entities in this illicit market, who do not see, know or meet each other, but who have developed a criminal system of drug trafficking hitherto unimaginable and unknown. "The trust among the participants in this trade was highlighted through reviews and ratings on the DarkNet's networks." (Morselli, Décary-Hétu, Paquet-Clouston & Aldridge, 2017; Munksgaard & Tzanetakis, 2022, p. 19). One of the important findings of numerous studies on this topic is the resistance of participants in the drug trade to bear the legal consequences when shutting down individual online markets where narcotics were bought and sold. The question is how many effects are achieved by shutting down individual online markets that deal in drug trafficking, "because participants in that trade very quickly migrate to some new networks and remain inaccessible to judicial authorities" (Ladegaard, 2019).

"The virtual nature of crypto drug markets has meant that participants in this market do not need to physically meet" (Aldridge et al., 2018). Some scholars note that before online drug trafficking, there was a much higher degree of criminalization on the streets, and that since the drug sale was registered in 2011, there have been far fewer clashes between criminal gangs, especially in the United States. Starting with Silk Road in 2011, "the number of crypto narcotics markets increased rapidly" (Christin, 2013), to an estimated "118 cryptomarkets in 2019 specializing in the sale of goods on the black market" (United Nations Office on Drugs and Crime, 2021). " Cryptomarkets are now an important source of supply of drugs for personal use and sale to a wider range of people" (Demant, Munksgaard, Décary-Hétu & Aldridge, 2018). Online drug markets are trying to circumvent the laws by conducting their operations on the DarkNet while relying on cryptocurrencies such as Bitcoin to carry out transactions. The issue of trust is also an important aspect of the coordination problem: how can customers be sure that they will get quality "goods" for their money when they have no protection in case the product is of poor quality or simply if they are scammed?

In this regard, experience from legal online marketplaces is used, "so that a reputation system based on reviews and ratings of sellers is applied in crypto drug markets" (Przepiorka, Norbutas & Corten, 2017). On some cryptomarkets, "a system of depositing funds with third parties is also used, in order to prevent possible disputes between buyers and sellers, which overall contributes to greater trust among both buyers and dealers" (Munksgaard & Tzanetakis, 2022, p. 20). Shoppers in cryptomarkets "feel more secure compared to other forms of drug distribution" (Morselli et al., 2017).

Since the establishment of the first crypto drug market, *Silk Road*, in 2011, the number of anonymous online drug markets has expanded significantly, making online commerce a common method for buying and selling illicit substances (United Nations Office on Drugs and Crime, 2021). Numerous studies have examined drug trafficking through the DarkNet (Aldridge, Stevens & Barratt, 2018), including the coordination between buyers and sellers (Bakken, Moeller & Sandberg, 2018) and the mechanisms used to establish and maintain trust in these illicit markets. Despite the lack of direct interaction between participants,

they have developed a sophisticated system for drug trafficking that was previously unimaginable. Trust within this trade is reinforced through review and rating systems embedded in DarkNet platforms (Morselli, Décary-Hétu, Paquet-Clouston & Aldridge, 2017; Munksgaard & Tzanetakis, 2022, p. 19).

An important finding in research on this topic is the resilience of online drug markets despite legal interventions. Participants often evade legal consequences when individual platforms are shut down, as they quickly migrate to new networks that remain inaccessible to law enforcement (Ladegaard, 2019). The virtual nature of crypto drug markets eliminates the need for physical meetings (Aldridge et al., 2018). Some scholars suggest that prior to online drug trafficking, street-based distribution resulted in higher levels of criminal violence, whereas since the emergence of Silk Road in 2011, violent clashes among criminal gangs—particularly in the United States—have declined.

Following the launch of Silk Road, the number of crypto drug markets expanded rapidly (Christin, 2013), reaching an estimated 118 cryptomarkets in 2019 dedicated to black-market trade (United Nations Office on Drugs and Crime, 2021). Cryptomarkets have become a major source of drug supply, serving both personal users and larger distribution networks (Demant, Munksgaard, Décary-Hétu & Aldridge, 2018). These markets operate within the DarkNet and leverage cryptocurrencies such as Bitcoin to facilitate transactions while circumventing legal restrictions.

Trust is a crucial element in this illicit trade, as buyers lack formal protections against fraudulent or low-quality products. To address this issue, crypto drug markets borrow strategies from legal e-commerce platforms, incorporating reputation systems based on seller reviews and ratings (Przepiorka, Norbutas & Corten, 2017). Additionally, some cryptomarkets implement third-party escrow systems to mitigate disputes between buyers and sellers, further strengthening trust (Munksgaard & Tzanetakis, 2022, p. 20). Many shoppers perceive cryptomarkets as a safer alternative to traditional drug distribution methods (Morselli et al., 2017).

The increasing accessibility of illicit substances through online marketplaces has influenced consumption patterns. Research suggests that "drug buyers and users tend to consume drugs more often but also buy smaller quantities and generally engage in controlled consumption of illicit substances" (Barratt, Lenton, Maddox & Allen, 2016, p. 50). However, one of the primary vulnerabilities of DarkNet platforms is the risk of market shutdowns, which can occur in four distinct ways.

First, voluntary closures take place when cryptomarket administrators shut down their platforms and return deposited funds to users, typically due to unprofitability or fear of law enforcement intervention. Second, exit fraud occurs when administrators abruptly shut down the market without prior notice, retaining all deposited funds (Barratt, 2012, p. 683). Third, DarkNet marketplaces may be hacked, with attackers either stealing deposited funds or exposing market operations for unknown reasons. Finally, markets may be **seized by law enforcement,** leading to asset confiscation—often in the form of Bitcoin—as well as the arrest and prosecution of administrators.

The frequent and unexpected shutdowns of DarkNet platforms pose a significant threat to the stability of the online drug trade. "The unexpected shutdowns of platforms on the DarkNet pose a major threat to the stability of the online drug market. Specifically, between 2011 and 2016, 88 DarkNet platforms were opened, of which 82 were closed before the end of 2016" (Barratt et al., 2016, p. 56). Despite these disruptions, administrators and users have adapted by rapidly migrating to new platforms, treating shutdowns as temporary setbacks rather than insurmountable obstacles to the continuation of online drug trafficking.

2.1. DarkNet: The dark side of the Internet as a hub of online drug trafficking

DarkNet marketplaces, also known as cryptomarkets, facilitate illegal online trade through platforms "similar to legal online platforms that facilitate trade, such as eBay or Amazon" (Munksgaard & Tzanetakis, 2022, p. 20). These platforms leverage encryption technologies alongside user-friendly interfaces, allowing "illicit trades to take place

on easy-to-use platforms without any direct encounter and with anonymous identities and locations, making the DarkNet a breeding ground for illicit trades" (Tzanetakis, 2018). As the DarkNet market continues to expand, international cooperation and information exchange among law enforcement agencies remain critical to combat its exponential growth (Reitano, 2015). Most activity on DarkNet marketplaces revolves around illicit drug trafficking, making it a central pillar of this hidden economy (Europol, 2017).

One of the primary reasons buyers are drawn to DarkNet markets is their perception of a safer environment for drug purchases; "due to the absence of personal contact with dealers, erasing all kinds of risks of potential violence" (Barratt et al., 2016, p. 57). However, while anonymity protects sellers, buyers must still provide a delivery address, which introduces vulnerabilities such as potential exposure of personal information, fraud, blackmail, or identification by law enforcement authorities (Europol, 2017).

Additionally, DarkNet platforms enable drug dealers to expand their customer base beyond their immediate physical territory, overcoming geographical limitations that would exist in traditional street-level markets due to competition and territorial disputes among rival dealers (Morselli et al., 2011). These dealers operate with a high degree of identity protection, relying on encryption and anonymity mechanisms built into DarkNet marketplaces. However, customer trust is also reinforced through feedback and rating systems, mirroring those found in legitimate online marketplaces.

To fully grasp the functioning of online drug markets, it is essential to define and distinguish key concepts frequently encountered in this discourse, including the DarkWeb, DarkNet, and Tor—each playing a distinct role in the ecosystem of illicit online trade.

The dark web (or *Dark Web*) is "a piece of the internet consisting of hidden sites that cannot be found through conventional and well-known web search engines" (Guccione, 2021). Instead, it is necessary to install a publicly available Tor browser through which the Tor network is accessed, which provides anonymity to the user when performing web traffic.

The Dark Net (or *DarkNet*) is "a small part of the Dark Web that is designed for people to communicate anonymously. Commonly known as the DarkNet ("dark or hidden web"), this hidden part of the internet is considered a space for criminal activity" (Buxton & Bingham, 2015, p. 12). In addition, almost everyone has heard stories of drug and human trafficking or even murders that have been organized on the dark web. Regular search engines, such as Google, Bing, etc., can't find websites from the DarkNet. Sites on the DarkNet can only be accessed by using the Tor network. Sites, i.e. hidden or onion services, can only be accessed if the exact URL, whose domain name ends in .onion, is known. The DarkNet is actually a place to trade all kinds of illegal goods, and payment is mostly made in cryptocurrencies. Since there is no way to track users, communication over *the Darknet* provides the highest security and privacy. Due to the encrypted communication and anonymity it provides, criminals make maximum use of the DarkNet. The risk of malware spreading is much higher here than on ClearNet. Visitors to the DarkNet can easily fall for suspicious offers or come into contact with criminal organizations and thus become vulnerable to criminal prosecution. Browsing the DarkNet itself is not illegal, although it does pose a security risk. As soon as a person downloads illegal content on their computer, or buys illegal goods and services, they become a criminal. The sale of illegal goods and services is also punishable. In this regard, "the DarkNet is not really different from the physical world: what is illegal offline is still illegal on the Internet, regardless of whether it is on the ClearNet or the DarkNet" (Buxton & Bingham, 2015, p. 12).

As you can see from the name of the network, the DarkNet is the darkest place on the Internet and abounds in illegal content. On the DarkNet, you can most often find sites for the sale of drugs, sites that sell child pornography, then various types of weapons and military equipment (pistols, rifles, bombs, although it is also possible to order hand launchers and other weapons). Also, the DarkNet provides the ability for people to buy fake identities, stolen goods, and various information. It is possible to organize and order a robbery, and there are cases where a murder has been ordered through this network.

The Dark Web refers to a segment of the internet that consists of hidden sites inaccessible through conventional search engines such as Google or Bing (Guccione, 2021). Accessing these sites requires the installation of specialized software, such as the publicly available Tor browser, which enables users to browse the Tor network while maintaining anonymity.

Within the Dark Web exists a smaller, more restricted subset known as the DarkNet, designed for anonymous communication and often associated with illicit activities (Buxton & Bingham, 2015, p. 12). While mainstream search engines cannot index DarkNet sites, users can access them through the Tor network. These sites, referred to as onion services, require exact URLs ending in ".onion" to enter.

The DarkNet facilitates the trade of various illegal goods, with transactions typically conducted using cryptocurrencies to preserve anonymity. Due to its encrypted communication channels, criminals exploit the DarkNet for illicit transactions, making it a breeding ground for cybercrime. However, its inherent risks extend beyond law enforcement detection—malware proliferation is significantly higher than on the ClearNet (the publicly accessible internet), exposing users to potential security threats.

Importantly, browsing the DarkNet itself is not illegal, but engaging in illegal activities—such as downloading illicit content, purchasing illegal goods or services, or facilitating cybercrime—constitutes a criminal offense. The DarkNet operates similarly to the physical world: activities deemed illegal offline remain illegal online, regardless of whether they occur on the ClearNet or DarkNet (Buxton & Bingham, 2015, p. 12).

DarkNet is the darkest place on the Internet and abounds in illegal content. DarkNet marketplaces frequently host sites dedicated to the sale of drugs, weapons, child pornography, counterfeit identities, and stolen goods. Reports have also highlighted its involvement in organizing cybercrime, fraud, and, in rare instances, more severe offenses such as contracted violence, even murder.

Tor ("The Onion Routing") is a modified version of the Mozilla Firefox browser designed to protect user anonymity by concealing their IP address, location, and other identifying information from conventional

websites (Swan, 2016, p. 110). Originally developed by the U.S. Navy's research department, Tor continues to receive funding from the U.S. government. Its name—an acronym for "The Onion Router"—reflects its multi-layered encryption process, which ensures that only those with the appropriate decryption key can access the original data (Swan, 2016, p. 111).

This encryption model is similar to the security protocols used in the banking sector and online commerce, where intercepted emails or transactions remain unreadable without proper authorization. Tor achieves anonymity by routing internet traffic through multiple intermediaries, known as Tor relays—typically three relays for communication with ClearNet web servers and up to six for interactions with onion services. Through this process, encrypted communication appears random to external observers, as traffic is transmitted across multiple global servers before reaching its destination.

The Tor browser and its associated sites are widely used within the DarkNet, identifiable by the ".onion" domain. Unlike ClearNet URLs, onion service addresses cannot be mapped to an IP address, making it significantly more difficult for investigators to locate them. Furthermore, even when DarkNet marketplaces are seized by law enforcement, the IP addresses of web clients—including sellers and buyers—remain inaccessible to web servers, ensuring continued anonymity.

2.2. The impact of the COVID-19 pandemic on online drug sales

The COVID-19 pandemic disrupted multiple aspects of social life worldwide, including its effects on various vulnerable populations, such as drug users. While some research suggests that economic recessions generally do not reduce narcotics demand, as drug users tend to be consistent consumers (Caulkins, 2011), other studies indicate that certain extreme circumstances can lead to shifts in drug markets (Dunlap, Graves & Benoit, 2012). Although the pandemic did not significantly alter overall demand for illicit substances, it created substantial distribution challenges, particularly for international shipments.

Following the outbreak of COVID-19, the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) noted increased traffic in cryptomarkets, raising questions about whether these platforms had become more viable channels for drug distribution, given the absence of face-to-face transactions (EMCDDA, 2020). Drug traffickers who previously concealed narcotics within **l**egitimate international shipments (United Nations Office on Drugs and Crime, 2020) faced new logistical obstacles due to border closures aimed at curbing the spread of the virus. As a result, international drug trafficking became increasingly difficult—if not temporarily halted—due to travel and trade restrictions.

The pandemic's impact on illicit drug markets varied depending on both the geographic location of sellers and buyers, as different regions experienced varying degrees of disruption (United Nations Office on Drugs and Crime, 2020). While international cryptomarket transactions faced significant obstacles, domestic cryptomarkets may have been less affected. The type of drug being sold also played a role in market shifts; for instance, reports from EMCDDA and Europol suggested that COVID-19 had minimal impact on cocaine sales but led to a decline in demand for synthetic drugs (EMCDDA-Europol, 2020). Furthermore, drug prices for most substances increased in cryptomarkets post-pandemic, likely as a result of supply shortages rather than shifts in consumer behavior (EMCDDA-Europol, 2020).

Since many cryptomarket participants are based in Western industrialized nations, the pandemic may have disrupted major players in online drug markets, weakening their competitive advantage. The Netherlands, recognized as a leading supplier of illicit drugs in cryptomarkets (EMCDDA-Europol, 2019), saw a notable decline in its presence following the outbreak (EMCDDA-Europol, 2020), reflecting broader market instability.

3. Law Enforcement Efforts Against Online Drug Trafficking

Globally, law enforcement agencies have primarily targeted the operators of online drug markets, focusing on prosecuting the owners

of DarkNet platforms and shutting down cryptomarkets. One of the key strategies involves direct market disruption, with police agents infiltrating illicit platforms by posing as both buyers and sellers. This approach has increased transaction costs and, more importantly, undermined the trust that previously existed between online buyers and dealers. In some cases, officers have instilled further suspicion among sellers by posting fake negative reviews, discouraging transactions (Hutchings & Holt, 2017).

Additional enforcement measures include stricter controls on financial transactions and prosecuting both buyers and dealers exposed through these efforts. However, online drug trade has proven highly resilient to legislative interventions. DarkNet markets remain highly interconnected, allowing users to migrate quickly to new platforms when existing ones are shut down—ensuring that such disruptions have a minimal impact on overall drug prices (Ouellet, Maimon, Howell & Wu, 2022, p. 1518).

The use of DarkNet marketplaces for drug trafficking remains a global issue, with significant growth in recent years—especially in India and Southeast Asian countries, including Indonesia, Thailand, and Vietnam (United Nations Office on Drugs and Crime, 2020). As cryptomarkets continue to evolve, law enforcement agencies worldwide face ongoing challenges in effectively dismantling these platforms and mitigating their influence on international drug trade networks.

4. Methods of Distributing Drugs Purchased Through the DarkNet

While technological innovations have enhanced anonymity in DarkNet marketplaces, drug delivery remains a critical vulnerability, as law enforcement can intercept shipments containing narcotics. To mitigate these risks, buyers in Western countries employ several strategies to avoid detection. These include selecting delivery locations far from home or work, regularly rotating addresses, avoiding postal services that require signatures, and even using real customer names to make packages appear less suspicious (Aldridge & Askew, 2017, p. 102).

Despite these precautions, substances sent via mail are always at risk of seizure. However, interception alone does not necessarily identify the sender, nor does it provide definitive proof that the recipient knowingly purchased drugs online. Sellers further protect their anonymity by excluding return addresses on packages, allowing buyers to claim that any seized drugs were delivered in error (The Washington Post, 2018). Additionally, since mail containing drugs often appears indistinguishable from regular parcels, most shipments do not undergo thorough security checks.

Another distribution method, used less frequently in Western countries but widely adopted elsewhere, is dead drop delivery (Aldridge & Askew, 2017, p. 104). This approach eliminates reliance on postal services and significantly reduces delivery delays, making it a preferred method in many regions.

The online drug trade is more efficient than traditional street markets, exhibiting lower rates of theft and fraud (Bhaskar, Linacre & Machin, 2019). This increased efficiency stems from several technological advancements that enhance market transparency and competition.

One of the major challenges of street-based drug trafficking is the information asymmetry between buyers and sellers regarding drug quality. Illicit street drugs are often mixed with adulterants—including baking soda, sugar, starch, painkillers, talc, milk powder, laundry detergent, caffeine, and even rat poison—which compromises purity and increases health risks (American Addiction Centers, 2019). Consumers purchasing drugs on the street lack the ability to verify quality or file complaints, making fraud and contamination common concerns.

DarkNet marketplaces address these problems by implementing buyer and seller feedback systems, similar to those found on legal e-commerce platforms such as eBay. These systems incentivize vendors to offer higher-quality drugs, as future sales depend on positive customer reviews (Espinosa, 2019, p. 29).

Additionally, the "escrow" system plays a crucial role in ensuring transactional integrity. In this model, DarkNet platforms hold funds until buyers receive their goods. Once the purchase is confirmed, the platform releases the payment to the seller, minimizing fraud and protecting buyers from unreliable dealers.

Since goods on DarkNet marketplaces are paid for upfront, buyers face a significant risk that sellers may fail to deliver the product after receiving payment—a common concern in transactions involving illegal goods. While some platforms implement depositing systems to mitigate fraud, participation in these systems is optional. In certain cases, buyers prefer to pay sellers directly to expedite transactions—a practice known as "Finalize Early", which is typically reserved for trusted sellers (Darknetone, 2021).

It is important to note that feedback and escrow systems were not pioneered by DarkNet markets. Such mechanisms have long been integral to legal online marketplaces such as eBay, Airbnb, and Amazon, where positive feedback plays a crucial role in determining reputation and pricing (Anderson & Magruder, 2012). The escrow system, first implemented by Amazon, has proven effective in enhancing trust between buyers and sellers (Paulou & Geffen, 2004, p. 40).

Trust remains a central issue in online drug sales, given the ethical and legal complexities of the narcotics trade. Buyers often lack certainty regarding the quality of substances until they have used them, creating opportunities for sellers to engage in fraudulent practices, such as mixing drugs with cheaper, low-quality substances.

For buyers seeking reliable connections, the key challenge is identifying sellers who aim to maximize long-term profitability by fostering consistent customer relationships. Only after experiencing a product firsthand do buyers decide whether to continue purchasing from the same seller or seek alternatives.

5. Research on the Operation of DarkNet Platforms for Online Drug Sales

Since their emergence in 2011, DarkNet marketplaces have facilitated the sale of various illegal goods and services, including drugs. Many of these platforms have operated for brief periods before being shut down. Among the most well-known examples are Silk Road, which launched in the United States in 2011, and Hydra, Russia's dominant

DarkNet marketplace. This paper examines the operational structures of these platforms and the mechanisms that sustained their illicit drug trade. Both Silk Road and Hydra were ultimately dismantled—Silk Road in 2013 and Hydra in April 2022—after prolonged evasion of law enforcement.

Silk Road served as the first modern DarkNet marketplace, enabling anonymous transactions for illegal goods and services. Founded by Ross Ulbricht in 2011, it relied on two key technologies to protect user anonymity: the Tor network and Bitcoin (Martin, 2013, p. 351). Bitcoin, introduced in 2009, provided a decentralized currency system that operated without oversight from banks or governments. The security of transactions was ensured through blockchain technology, which records data in sequentially linked blocks, preventing unauthorized modifications (Martin, 2013, p. 353).

Blockchain technology facilitated Silk Road's order processing, payments, and transaction tracking. This system maintained transaction integrity by preventing unauthorized modifications, thus ensuring a transparent record of exchanges. Silk Road hosted a diverse range of illegal products, though by 2013, nearly 70% of purchases were drug-related. The platform's reliance on postal shipments ultimately led to its downfall, as authorities traced and intercepted deliveries, allowing U.S. law enforcement to apprehend Ulbricht's associates and shut down the marketplace (Martin, 2013, p. 358).

Despite the anonymity provided by the Tor network, law enforcement initially struggled to identify the mastermind behind Silk Road. However, U.S. federal agents (FBI) ultimately traced its operations to Ross Ulbricht through a fortunate discovery. Reports suggest that Silk Road's IP address was inadvertently exposed on a Reddit forum, making it visible online. Agents investigated these claims by posting data on Silk Road and utilizing traffic analysis software to pinpoint the IP address (Lacson & Beata, 2016, p. 40).

Ulbricht, operating under the alias "The Dread Pirate Roberts," accessed the network from a public library, which led to his identification and arrest. He was subsequently charged with money laundering, computer hacking, drug trafficking, and conspiracy to murder at least five

individuals who allegedly posed a threat to exposing Silk Road's operations. Following trial proceedings, Ulbricht was convicted and received five sentences, including two life sentences without the possibility of parole, along with a $183 million fine (Lacson & Beata, 2016, p. 40).

While much of the discourse surrounding online crime focuses on Western enforcement strategies, the largest DarkNet drug market experienced its most significant expansion in Russia, where the Hydra marketplace operated for seven years. Since its inception in 2015, Hydra evolved into a highly sophisticated platform, with virtually no competition, making it the largest cryptomarket for drug trafficking worldwide (VICE, 2020).

Unlike Western law enforcement agencies, Russian authorities demonstrated limited commitment to shutting down Hydra. While individual couriers were occasionally arrested (VICE, 2020), the main organizers operated freely, allowing Hydra to expand annually, cementing its dominance in the illicit market. No other DarkNet drug marketplace sustained operations for as long as Hydra, which was ultimately shut down in April 2022 after years of evading prosecution.

Hydra enabled anonymous communication between wholesalers, dealers, and end users, facilitated by cryptocurrency payments and a dead-drop delivery system. The platform's self-regulated marketplace included an advertising framework for sellers, as well as reviews and rating mechanisms, ensuring a structured market for illicit transactions. The digitalization of the drug trade, amplified by Hydra's sustained presence, led to a notable increase in the share of online drug trafficking.

Hydra's reach was extensive—its activity spanned 1,129 settlements across every Russian region, covering 69% of the population (Goonetilleke, Knorre & Kuriksha, 2023, p. 735). Larger cities housed a higher concentration of vendors, with broad inventories of narcotics available for sale. Expensive drugs were primarily distributed in wealthier districts, particularly business areas, reflecting the platform's highly competitive nature, both at regional and national levels (Goonetilleke, Knorre & Kuriksha, 2023, p. 736).

The Russian government acknowledged Hydra's role in the drug trade only in 2019, though its closure occurred solely through U.S. and

German intervention. The U.S. government estimated that Hydra facilitated over $5 billion in illicit transactions from 2016 to 2022, accounting for 80% of all DarkNet cryptocurrency transactions in 2021 (United States vs. Pavlov, 2022). The U.S. Department of Justice recognized Hydra as the largest and longest-running DarkNet marketplace globally (United States vs. Pavlov, 2022).

While Hydra remained Russia's dominant drug marketplace, smaller illicit trade hubs—operating via Telegram bots and groups—also existed but were limited to localized transactions. Reports confirm that Hydra was the preferred platform for illegal drug purchases, particularly in Moscow, St. Petersburg, and other major cities. Compared to Western DarkNet platforms, Hydra uniquely operated for seven years without major legal interference. Unlike other marketplaces that rarely survived beyond a year, Hydra's longevity allowed it to develop a structured regulatory framework, introduce quality assurance mechanisms, and implement secure transaction models, reinforcing its influence in the Russian drug trade.

A defining feature that distinguished Hydra from other DarkNet marketplaces in the United States and Europe was its delivery method. Most DarkNet platforms rely on mail-order transactions, with suppliers using postal services or private couriers to disguise drug shipments. However, after Russia introduced a law in 2014 requiring postal inspections for illicit substances, this method became less viable, prompting Hydra to develop an alternative approach.

Instead of postal services, Hydra operated through a dead-drop delivery system, eliminating direct exchanges between buyers and sellers. Before a transaction took place, couriers would conceal drugs in various locations across cities. Sellers listed the type, quantity, approximate location, and price of each item on Hydra's website, allowing buyers to browse availability prior to purchase. Once payment was completed, buyers received precise retrieval instructions, detailing the location of the concealed package.

Hydra employed several methods for hiding drug shipments. One technique involved attaching packages to surfaces using magnets, making them difficult to detect. Another approach required burial in the ground, particularly in parks or public areas, while in colder months,

the same method was adapted by burying drugs in snow. Some packages were simply hidden in discreet locations where accidental discovery was unlikely. Additionally, Hydra facilitated pre-order transactions, where customers could purchase wholesale quantities or rare substances, which were concealed only after payment had been finalized.

The marketplace's remote and encrypted communication system between administrators, sellers, couriers, and buyers helped reduce legal risks associated with illicit drug transactions. However, the dead-drop method carried inherent vulnerabilities, as law enforcement could monitor public locations for suspicious activity, such as individuals digging in parks or searching in concealed areas. These behaviors often signaled drug retrieval, increasing the likelihood of detection.

Like other DarkNet markets, Hydra allowed vendors to register and list various narcotics for sale. The marketplace was structured into three key roles: administrators, operators, and couriers. Administrators managed platform settings, financial transactions, and personnel assignments, while operators oversaw customer disputes and mediated interactions. Couriers played a direct role in delivery, ensuring the drugs reached their intended locations.

Customers could anonymously browse Hydra's listings, filtering available substances by drug type, seller, location, price, and quantity. Hydra incorporated a review and rating system similar to those found in legal e-commerce platforms, allowing buyers to assess product quality and vendor reliability. Transactions were conducted exclusively through Bitcoin, with users given two deposit options—either purchasing Bitcoin externally and transferring it to Hydra's market address or using alternative payment methods designed to avoid direct financial institution involvement.

Another payment method available on Hydra was the KIWI wallet, a service provided by the Russian financial company KIWI. This system allowed users to deposit cash at ATM-like terminals across Russia, converting it into Bitcoin, which could then be used for transactions on the platform. Since these terminals did not require identification, this method ensured a high level of anonymity for customers (Goonetilleke et al., 2023, p. 738). The accessibility of KIWI terminals simplified cryp-

tocurrency transactions, making them more convenient compared to Western alternatives.

Once a purchase was completed, Hydra employed an escrow system, holding funds until the transaction was confirmed as successful. Upon payment verification, buyers received detailed information about the drug's dead-drop location, including photos and GPS coordinates for retrieval. This method eliminated the need for physical contact between sellers and buyers, reinforcing the platform's anonymity model (Goonetilleke et al., 2023, p. 738). Additionally, all communication between buyers and sellers took place within the encrypted Tor network, ensuring that financial transactions remained untraceable when processed through Bitcoin or cash deposits at KIWI terminals.

To further enforce security and platform exclusivity, Hydra imposed strict communication rules, prohibiting interactions outside its system. Violations, such as attempting to communicate externally, resulted in a 2 Bitcoin penalty for sellers, while buyers who reported such attempts were rewarded (Saidashev & Meylakhs, 2021, p. 175).

Hydra incorporated an automated review system, requiring customers to leave feedback within 24 hours of making a purchase. The platform's rating system ranged from 0 to 10, with most reviews being overwhelmingly positive. The average rating remained close to 10, while only 4% of orders received scores below this threshold. If a buyer failed to post a review within the given timeframe, Hydra automatically assigned a perfect score, artificially inflating vendor ratings (Goonetilleke et al., 2023, p. 738).

Beyond numerical ratings, buyers could leave written reviews detailing product quality, transaction issues, and potential discrepancies between advertised and delivered goods. Reviews were restricted to verified purchases, preventing fraudulent feedback from competitors.

Hydra allowed customers to file disputes if dissatisfied with the purchasing process or the quality of the goods received (Saidashev & Meylakhs, 2021, p. 176). Disputes typically arose from deliveries that failed to arrive at the specified location or were inaccessible due to police presence. Some issues stemmed from low-quality products or items that deviated from their advertised description.

Initially, buyers and sellers attempted to resolve disputes privately via Hydra's internal messaging system, often leading to refunds, discounts on future purchases, or product replacements. If an agreement could not be reached, a moderator intervened, reviewing the conversation history before making a final decision. Moderators usually ruled in favor of buyers, particularly if they had a history of legitimate transactions with minimal disputes (Goonetilleke et al., 2023, p. 738).

One distinguishing feature of Hydra was its seller ranking system, which allowed vendors to attain special statuses that enhanced their credibility and improved business operations. The Trustworthy Seller status could be purchased if the vendor met specific criteria, including at least 1,000 sales and a dispute rate below 7%. This designation increased customer confidence, improved search ranking visibility, and granted sellers greater authority over dispute resolution before cases were escalated to Hydra's moderators (Goonetilleke et al., 2023, p. 738). Additionally, trusted sellers were permitted to franchise, collaborating with smaller partners who manufactured synthetic drugs or marijuana, or acting as intermediaries in Hydra's marketplace (Saidashev & Meylakhs, 2021, p. 177).

Hydra's revenue streams were structured around monthly fees, commissions, and premium services. Sellers were required to pay both a flat monthly fee and a percentage-based commission on transactions. Additionally, Hydra monetized its homepage bidding system, where sellers could pay for top search rankings. The platform also profited from the sale of premium statuses to larger vendors. As of March 19, 2022, the cost to open a new store on Hydra was approximately $300, with an additional monthly rental fee of $100 (Goonetilleke et al., 2023, p. 740).

On April 5, 2022, Hydra was shut down when German law enforcement seized its servers in a joint operation with U.S. federal agencies (Bloomberg, 2022; Wall Street Journal, 2022). The Federal Criminal Police Office of Germany stated that the investigation had begun in August 2021 (Bundeskriminalamt, 2022). On the same day, the U.S. Department of the Treasury issued sanctions against Hydra (U.S. Department of the Treasury, 2022), and the U.S. Department of Justice indicted its alleged administrator (United States vs. Pavlov, 2022). No evidence has

surfaced suggesting that Russian authorities were involved in Hydra's takedown.

Despite speculation that Hydra would resurface on the DarkNet, the marketplace remained defunct for over a year, leading its former users to seek alternatives. In the immediate aftermath, buyers and sellers attempted to trade on DarkNet forums such as LegalRC and RuTor, while others migrated to newer marketplaces that lacked Hydra's extensive infrastructure and user base. Among the platforms that gained traction after Hydra's shutdown, the largest were OMG, Blacksprut, Mega, and Solaris (Chainalysis, 2023). Another marketplace, Kraken, launched in December 2022, positioning itself as Hydra's successor and reportedly operated by former Hydra affiliates.

6. Conclusion

The global fight against online drug trafficking requires strong international cooperation, as encryption and anonymity technologies continue to advance, enabling cybercriminals to evade detection. Law enforcement agencies worldwide are strengthening collaborative efforts to combat these illicit activities, recognizing that online drug sales transcend national borders. Advances in technology and data analysis have empowered security agencies to track online activities, identify digital traces, and expose participants in illegal transactions. As these technologies evolve, they may also help law enforcement counter encryption methods used to obscure drug trafficking networks.

Artificial intelligence plays an increasingly critical role in analyzing complex datasets and assisting security agencies in investigations. Online platforms, financial institutions, and service providers hold valuable information that can aid law enforcement in identifying and tracking drug dealers. Additionally, public awareness campaigns highlighting the dangers of purchasing drugs online can reduce demand, making it more difficult for criminal organizations to operate profitably.

The case of Hydra illustrates how a DarkNet marketplace, if left unchecked, can expand rapidly, achieving high levels of sophistication

and market dominance. Given the limited resources available to law enforcement, assessing the long-term impact of shutting down DarkNet platforms is essential. Many DarkNet marketplace users—both buyers and sellers—acquire the necessary expertise to navigate illicit platforms, enabling them to migrate seamlessly when a major market is dismantled. If large-scale DarkNet platforms encourage new users to learn how to operate in these environments, their influence may persist even after enforcement actions. Allowing such markets to expand unchecked could ultimately erode law enforcement's ability to contain online drug trafficking. While narcotics agencies continuously monitor criminal networks, the closure of major marketplaces often has minimal long-term effects, as illicit transactions rapidly shift to alternative platforms, causing overall sales to recover over time.

This research underscores the dedication of those who have relentlessly fought against organized crime, even at great personal cost. Italian judge and prosecutor Giovanni Falcone, a symbol of resistance against the mafia, famously argued that crime is not invincible but rather a system that can be dismantled. His words remind us that society must take a firm stance against organized crime by exposing its underlying mechanisms and challenging its perception of invulnerability. Falcone believed that justice, upheld through accountability and the rule of law, serves as a beacon of transparency, illuminating even the darkest sectors of criminal enterprise. His assertion that "the mafia thrives in darkness, but justice brings light" remains deeply relevant in the modern fight against crime, particularly within the hidden networks of the DarkNet.

To effectively combat online drug trafficking, criminal police and security services must maintain coordinated efforts that prioritize information sharing, advanced data analysis, and strategic infiltration of illicit online communities. Legislative frameworks must evolve to address the complexities of digital drug markets, including harsher penalties for offenders and international agreements fostering joint investigations. While strong legal measures are essential, they must be integrated into a broader strategy that includes technological innovation, criminal intelligence, and public awareness. By uniting all available legal and technological tools, authorities can reinforce the fight against online drug trafficking, ensuring that justice prevails against the evolving landscape of organized crime.

References:

Journal Articles:

Aldridge, J., Askew, R., (2017). Delivery dilemmas: How drug cryptomarket users identify and seek to reduce their risk of detection by law enforcement. *International Journal of Drug Policy*, 41, pp. 101–109. doi:10.1016/j.drugpo.2016.10.010

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

Anderson, M. & Magruder, J. (2012). Learning from the Crowd: Regression Discontinuity Estimates of the Effects of an Online Review Database, *The Economic Journal*, 122, Issue 563, pp. 957–989, https://doi.org/10.1111/j.1468-0297.2012.02512.x

Bakken, S. A., Moeller, K. & Sandberg, S. (2018). Coordination problems in cryptomarkets: Changes in cooperation, competition and valuation. *European Journal of Criminology*, 15 (4), pp. 442–460. doi:10. 1177 /1477370817749177

Barratt, M., (2012). Silk Road: Ebay for drugs, *Addiction*, Abingdon, England, 107, available at: https://doi.org/10.1111/j.1360-0443.2011.03709.x

Barratt, M., Simon Lenton, J., Maddox, A. & Allen, M. (2016). What if you live on top of a bakery and you like cakes? - Drug use and harm trajectories before, during and after the emergence of Silk Road. *International Journal of Drug Policy*, 35, pp. 50–57. doi:10.1016/j.drugpo.2016.04.006

Bhaskar, V., Linacre, R. & Machin, S. (2019). The economic functioning of online drugs markets, *Journal of Economic Behavior & Organization*, 159, pp. 426–441.

Buxton, J. & Bingham, T. (2015). "The rise and challenge of dark net drug markets." *Policy brief*, 7.2, pp. 1-24.

Caulkins, J., (2011). The global recession's effect on drug demand - Diluted by inertia. *International Journal of Drug Policy*, 22, pp. 374–375. 10.1016/j.drugpo.2011.02.005.

Christin, N., (2013). Traveling the silk road: A measurement analysis of a large anonymous online marketplace. *In Proceedings of the 22nd international conference on World Wide Web*, pp. 213–224, doi:10.1145/2488388.2488408

Demant, J., Munksgaard, R., Décary-Hétu, D. & Aldridge, J. (2018). Going Local on a Global Platform: A Critical Analysis of the Transformative Potential of Cryptomarkets for Organized Illicit Drug Crime. *International Criminal Justice Review*, 28 (3), pp. 255–274. doi:10.1177/1057567718769719

Dunlap, E., Graves, J. & Benoit, E. (2012). Stages of drug market change during disaster: Hurricane Katrina and reformulation of the New Orleans drug market, *International Journal of Drug Policy*, 23, pp. 473–480. 10.1016/j.drugpo.2012.04.003

EMCDDA-Europol. (2019). EU Drug markets report 2019, Luxembourg, *Publications Office of the European Union*.

EMCDDA-Europol. (2020). EU Drug markets impact of COVID-19. Luxembourg, *Publications Office of the European Union*.

Espinosa, R. (2019), Scamming and the reputation of drug dealers on darknet markets. *International Journal of Industrial Organization*, 67.

Goonetilleke, P., Knorre, A. & Kuriksha, A. (2023). Hydra: Lessons from the World's Largest Darknet Market, *Criminology & Public Policy*, 22.4, pp. 735-777.

Hutchings, A. & Holt, J. T. (2017). The online stolen data market: Disruption and intervention approaches, *Global Crime*, 18 (1), pp. 11–30. doi:10.1080/17440572.2016.1197123

Ladegaard, I., (2019). Crime displacement in digital drug markets. *International Journal of Drug Policy*, 63, pp. 113–121. doi:10.1016/j.drugpo.2018.09.013.

Lacson, W. & Beata, J. (2016). The 21st century darknet market: lessons from the fall of Silk Road, *International Journal of Cyber Criminology*, 10.1.

Martin, J., (2013). Lost on the Silk Road: Online drug distribution and the 'cryptomarket'. *Criminology and Criminal Justice*, 14, pp. 351–367. doi.org/10.1177/1748895813505234

Morselli, C., Turcotte, M. & Tenti, V. (2011). The mobility of criminal groups. *Global Crime*, 12, pp. 165–188. doi.org/10.1080/17440572.2011.589593

Morselli, C., Décary-Hétu, D., Paquet-Clouston, M. & Aldridge, J. (2017). Conflict Management in Illicit Drug Cryptomarkets. *International Criminal Justice Review*, 27 (4), pp. 237–254. doi:10.1177/1057567717709498

Munksgaard, R. & Tzanetakis, M. (2022). Uncertainty and risk: A framework for understanding pricing in online drug markets. *International Journal of Drug Policy*, 101, doi:10.1016/j.drugpo.2021.103535

Ouellet, M., Maimon, D., Howell, C. J. & Wu, Y. (2022). The Network of Online Stolen Data Markets: How Vendor Flows Connect Digital Marketplaces, *The British Journal of Criminology*, 62 (6), pp. 1518–1536. doi:10.1093/bjc/azab116

Pavlou, P. & Gefen, D. (2004). Building effective online marketplaces with institution-based trust. *Information systems research*, *15*(1), pp. 37-59.

Przepiórka, W., Norbutas, L. & Corten, R. (2017). Order without Law: Reputation Promotes Cooperation in a Cryptomarket for Illegal Drugs, *European Sociological Review*, 33 (6), pp. 752–764. doi:10.1093/esr/jcx072

Reitano, T., (2015). Troels Oerting, Marcena Hunter, Innovations in International Cooperation to Counter Cybercrime. *The European Review of Organised Crime*, available at: https://globalinitiative.net/innovations-in-international-cooperation-to-counter-cybercrime/ (09.01.2024)

Saidashev, R. & Meylakhs, A. (2021). A qualitative analysis of the Russian cryptomarket Hydra, *Kriminologisches Journal*, 53, pp 169–185, doi:10.3262/KJ2103169

Swan, K., (2016). Onion routing and tor. *Geo. L. Tech. Rev*. 1.

Tzanetakis, M., (2018). Comparing cryptomarkets for drugs. A characterisation of sellers and buyers over time, *International Journal of Drug Policy*, 56, 176–186. doi:10.1016/j.drugpo.2018.01.022

Internet Sources

American Addiction Centers. (2019). What Is Heroin Cut With?, available at: https://americanaddictioncenters.org/heroin-treatment/cut-withl (04.01.2024).

Bloomberg, (2022). German Police Shut Down $1.3 Billion Illegal Darknet Firm [newspaper], available at: https://www.bloomberg.com/news/articles/2022-04-05/german-police-shutdown-1-3-billion-illegal-darknet-firm (05.01.2024).

Bundeskriminalamt. (2022). Illegal dark web marketplace "Hydra Market" shut down, [*release*], available at: https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2022/Presse2022/220405_PM_IllegalerDarknet-Marktplatz.html (04.01.2024).

Chainalysis. (2023). How Darknet Markets and Fraud Shops Fought for Users In the Wake of Hydra's Collapse, available at: https://blog.chainalysis.com/reports/how-darknet-markets-fought-for-users-in-wake-of-hydra-collapse-2022/ (04.01.2024).

Darknet. (2021). *Understanding Multisig vs. Escrow vs. Finalize Early on Darknet Markets*, available at: https://darknetone.com/understanding-multisig-vs-escrow-vs-finalize-early-on- darknet-markets/ (04.01.2024).

EMCDDA - European Monitoring Centre for Drugs and Drug Addiction. (2020). EMCDDA special report COVID-19 and drugs Drug supply via darknet markets, available at: https://www.emcdda.europa.eu/publications/ad-hoc/covid-19-and-drugs-drug-supply-via-darknet-markets_en. (25.12.2023).

Europol. (2017). How Illegal Drugs Sustain Organised Crime in the EU, available at: https://www.europol.europa.eu/publications-documents/how-illegal-drugs-sustain-organised-crime-in-eu (09.01.2024).

Guccione, D. (2021). What is the dark web? How to access it and what you'll find, (Jul 01, 2021), available at: https://www.csoonline.com/article/564313/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html (09.01.2024).

U.S. Department of the Treasury. (2022), Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex [*release*], available at: https://home.treasury.gov/news/press-releases/jy0701 (04.01.2024).

United Nations Office on Drugs and Crime. (2021a). *Darknet Cybercrime Threats to Southeast Asia* [report]. Available at: https://www.unodc.org/roseap/en/2021/02/darknet-cybercrime-southeast-asia/story.html (25.12.2023).

United Nations Office on Drugs and Crime. (2021b). Global overview of drug demand and drug supply [report]. Available at: https://www.unodc.org/unodc/en/data-and-analysis/wdr-2021_booklet-2.html (05.01.2024).

United States vs. Pavlov. (2022). United States District Court [*indictment*], available at: https://www.justice.gov/opa/press-release/file/1490906/download (05.01.2024).

The Washington Post. (2018). *Postal Service the preferred shipper for drug dealers*, available at: https://www.washingtonpost.com/politics/2018/10/16/postal-service-preferred-shipper-drug-dealers/ (26.12.2023).

MORE. (2020). *A New Breed of Drug Dealer Has Turned Buying Drugs into a Treasure Hunt*, available at: https://www.vice.com/en/article/g5x3zj/hydra-russia-drug-cartel-dark-web (04.01.2024).

Wall Street Journal. (2022). Russian 'Darknet' Market Tied to Ransomware Is Shut Down [*newspaper*], available at: https://www.wsj.com/articles/russian-darknet-market-tied-to-ransomware-is-shut-down-11649196069 (05.01.2024).