Committee: United Nations Office on Drugs and Crime

Topic: The Question of Enhancing Global Efforts to Prevent Illicit Drug Trade on the Dark Web

Student Officer: Hyoseok Choi

Position: Deputy Chair of UNODC

Introduction

In this current era of digitalization, the usage of the internet has increased over the years, leading to two types of webs—surface and deep webs—to appear. While surface webs are open and accessible to anyone, deep webs have a security process, mostly involving passwords. There are various licit activities happening on the deep web, such as online banking and paid services. However, not all deep websites are legal. Although the dark web, a type of deep web, can be reached using a normal connection, more rigorous security systems, such as systems that block the IP address, are installed on dark webs, meaning everyone using it is almost fully anonymous. This makes illegal activities freely happen in the dark web, with approximately 56% of all content found on the dark net outlawed, according to a statistical research conducted in 2020.

Dark webs fundamentally changed the operation of various illegal activities online, especially regarding illicit markets. As the internet makes the supply chains of products better, the trading of illegal goods on the dark web becomes a popular method. One of the most important products on the dark web is the illicit drug trade. The advantage of being anonymous makes these types of websites appealing to drug dealers and drug traffickers. In particular, the ability to trade even with no physical contact made trading more popular. Now, people can just click once, and the delivery will come right to their residence. Having said that, this aspect of dark web trading makes darknet markets a global issue. According to the European Monitoring Centre for Drugs and Drug Addiction, approximately 15% of global drug sales occur on darknet markets. In the future, this percentage may increase due to the ease of usage, market diversity, and the challenge of mitigating black market users in new marketplaces. It is also estimated that the global dark web market in general would reach $1.3 billion

by 2028, with an annual growth rate of 22.3%, meaning that more people would use darknet marketplaces.

Dark webs are also operated with the support of cryptocurrency. Yet, it is estimated that only between 0.1% to 1.9% of all cryptocurrency transactions involve illicit services and goods. By systematically investigating the existing blockchains of various cryptocurrencies of suspicious addresses performing illegal transactions, it is suggested that darknet markets grew in volume until 2021, with around $2.7 billion in volume, before declining by half around 2022. It is also worthwhile to mention that Silk Road, the first major darknet website to utilize both cryptocurrency and Tor, became the blueprint for many darknet marketplaces after its success in 2013.

According to an internet survey that was conducted in 10 European countries using various methods from 2017 to 2018, it showed that from 20,000 drug consumers who used the internet, 8% bought drugs on the dark net, which was significantly lower than drug dealers who accounted for 59% of consumers, but higher compared to other methods. During 2020 to 2021, this percentage doubled and grew to almost 15%. However, the most recent survey in 2022 had a result of 10% of total people buying drugs from darknet marketplaces. Although these are only a small sample, they suggest that black markets in the dark web have declined in general, as a result of stricter law enforcement and an increase in exit scams. Moreover, there are various international enforcement efforts currently happening. One of these examples is the multinational Operation SpecTor (2023), which was coordinated by Europol and the U.S. Department of Justice. It led to 288 arrests and over $53 million of assets and 850kg of drugs seized. Others include Operation DisrupTor (2020), where Europol, UNODC, and law enforcement agencies from around 9 countries cooperated, and Operation Dark HunTor (2021), which was the largest global darknet investigation during that time. Each operation usually had a giant success in closing down the major marketplace during that specific period, like Operation SpecTor shutting down Hydra Marketplace. These examples demonstrate that with global cooperation, the volume of darknet markets can decline further.

Definition of Key Terms

Dark Web

A certain type of network that can be only recognized by joining from a certain network or software, which cannot be found by standardised search engines such as google. The method of accessing the dark web includes software such as Tor (Onion Router), I2P, and Freenet. Since darkwebs are not indexed, standard search engines like Chrome and Safari cannot enter darkwebs. Each dark web website URL ends with a domain name associated with the software used. These programs have a general principle of rerouting the encrypted data in the dark web through other computers using the same software, which then disguises the origin and the destination of the data.

Not all acts on the dark web are outlawed. There are legal activities happening on the dark web, such as whistleblowing, which is informing other players about illegal activities that are happening inside the country. Other kinds of legit activities happening include journalism, especially when acquiring information in nations with high censorship. However, in general, the dark web is considered to be a treacherous place that should be carefully approached. Some of the key concerns include cybercrime, illegal activities, scams, malware, and illegal markets, and these are just a few examples of what is taking place inside the dark web.

Although joining the dark web itself is not a crime in countries such as the United States, United Kingdom, Germany, and Canada, it does not mean that people are encouraged to join the dark web. Some countries with high censorship, such as China, Iran, and Russia, outlaw even accessing anonymous tools like the dark web by blocking browsers like Tor. Additionally, in virtually all nations, if people take any actions when they are in the dark web, such as performing illicit behaviors and purchasing illicit goods, it will be penalized. Nevertheless, the level of punishment largely varies between nations.

Deep Web

Parts of the internet that is inaccessible in standard search engines. Deep webs consist of non-indexed pages, which are pages that are not included in the search engine, fee-for-service sites, private databases (such as email inboxes and credit card accounts), dark web, and more. It is expected

that the deep web is significantly bigger than the surface web, with approximately 90% of all websites in the internet existing in the dark web.

People commonly mistake the deep web for the dark web. However, the two of them are not the same. While the deep web is all of the internet that cannot be accessed using a search engine, the dark web is a part of the deep web that consists of websites with the primary purpose of performing illicit actions.

Surface Web

A general part of the internet that can be accessed using standardised search engines such as Google Chrome and Microsoft Bing. Reaching the surface web does not necessarily need any configuration, and it is generally easy to access. It is estimated that the surface web consists of only 5% of the total content available, although it comprises various popular '.com, .org, and .net' websites that many internet users mostly utilize. Although there are certain surface websites that try to track sites in the darknet, common browsers do not link directly to darknet websites.

Darkweb Marketplaces

A certain type of market that is available only on the dark web. Most of the marketplaces are only available via the Tor network (.onion sites). Although these websites are similar to most online marketplaces on the surface web, it is focused on maintaining users' anonymity, security, and decentralised trust. This made darknet marketplaces suitable for users to anonymously buy goods and services here, including banned and illegal goods like drugs.

Cryptocurrency

A digital currency generated by a public network, rather than a government, that uses cryptography to ensure payments are sent and received securely. The world's most used cryptocurrency is currently Bitcoin, and it is used in various places, including DeFi (decentralized finance), NFTs (Non-Fungible Tokens), and DApps (Decentralized Applications). In many darknet marketplaces, currencies used for payment are mostly in cryptocurrencies. Although the primary cryptocurrency used is mostly Bitcoin in many marketplaces worldwide, recently, an unrecognized coin called Monero has risen in use in various marketplaces.

Monero

A privacy-focused cryptocurrency designed to make transactions untraceable and unlinkable. Unlike many cryptocurrencies, such as Bitcoin and Ethereum, Monero's primary focus is on user privacy, which makes it preferable for darknet marketplaces over others.

Cybercrime

The use of a computer as a tool to perform illegal actions. This includes trafficking illicit goods such as drugs, stealing identities, violating privacy, and more. With the internet becoming a major factor in fields such as government and entertainment, cybercrime has grown in importance in this modern world. Law enforcement, especially for cybercrime, faces serious problems as it now requires national cooperation.

Black Market

An illicit market where goods and services are traded without government oversight. Goods typically include outlawed products, such as drugs and weapons, and legal items sold illegally, which include untaxed products. Black markets are often linked to organized crime, corruption, and exploitation.

Escrow

A financial agreement where assets are held by a third neutral party when two or more parties are in the process of completing a transaction. This third party holds the funds until the buyer and seller fulfill their contractual obligation. The escrow system is used in various places, such as real estate, the stock market, and online sales. Especially, in online transactions, the escrow system is becoming used more for high-value transactions, which leads to better security with just a small fee for both buyers and sellers.

Tor Network

A network that uses "Onion Router" to have anonymous connections to the internet. This allows users of the Tor Network to safely and anonymously access various content. Websites that can

be accessed only through Tor end in '.onion'. Tor networks hide both the user's IP address and the server's IP address, making connections anonymous.

Onion Routing

A key technology that is used in the dark web for security purposes. The term "Onion" refers to how data is wrapped in multiple layers of encryption, which is similar to the physical shape of onion layers.

Background Information

Creation of the Tor Network

The Tor network was first developed as “Tor Project” in the Naval Research Laboratory, which was a research institute of the U.S. Army. Approximately 85% of the total funding was from U.S. authorities, while the rest was from private sponsors and non-government organizations. The concept of onion routing was developed there during the mid-1990s. Its goal was to provide a free operation for anonymous connection data on the internet, while also trying to protect U.S. online communications. This was enabled by obscuring the sender and receivers from surveillance and analysis. Later, the first public version of Tor, also known as “The Onion Routing Project” at that time, was released.

How Darknet Marketplaces Work

Most darknet marketplaces are available only by using the Tor browser to prevent being tracked. There are various user roles inside darknet marketplaces. One of them includes admins, who control the general platform and manage the site. Another is sellers (or vendors), who offer diverse goods and services to the buyers.

There are a variety of products available from darknet marketplaces. The most popular category of products is drugs, but there are other products. They also offer online services, which are composed of hacking services, malware, DDoS attacks, and more. Some websites sell information that was stolen from others, including credit card information and fake passports or IDs. A more rare product includes physical weapons; however, they are heavily surveilled compared to others.

Darknet marketplaces use a wide range of payment methods, mostly focused on cryptocurrency. Currently, the most used cryptocurrency for payment is Bitcoin, as this allows users to be anonymous using its crypto wallet, which is unlike traditional systems. However, other types of cryptocurrency payment methods, such as Monero, are rising in use, with the benefits of better security and lower surveillance than Bitcoin, which is a popular cryptocurrency that is gradually rising in popularity.

Why Darknet Marketplaces are Preferred

It is estimated that around 10% of total drug users currently use the dark web for drug purchase, but this number is from a small sample of 20,000, meaning that there can actually be more potential users who primarily prefer darknet marketplaces over drug dealers and street markets. One of the reasons is ease of use. Unlike conventional methods that require face-to-face interactions, using darknet marketplaces mean that people do not have to physically risk their lives. With these low-risk environments, both users and sellers benefit from it. Additionally, darknet marketplaces often are global, meaning that people can have cheaper and better quality of product choices. These are also guaranteed and safe, with most of the marketplaces introducing escrow and review systems, which resemble online surface web marketplaces, and these kinds of benefits are hard to find in local drug vendors.

Use of Onion Routers in the Tor Network

The Tor network uses onion routers to ensure that the system is highly guarded and secured. The process of onion routing in the Tor network works as follows. When a user sends data inside the dark web, that data is encrypted multiple times. Then, it passes through 3 or more random Tor nodes. There are 3 types of nodes, which are entry nodes, middle nodes, and exit nodes. Entry nodes know the person of the data, however it does not know what the user is trying to access. Middle nodes only pass the information, and it cannot see the source or the destination of the data. Exit nodes decrypt the data and send the request to the internet. However, exit nodes cannot see the source of the data. This means that a single node cannot know both the person and what they are attempting. These nodes are primarily driven by volunteers, because of various reasons such as support for privacy, contribution to Tor, and community recognition. Nevertheless, running these nodes has a high cost of maintaining up to hundreds of gigabytes per month, and especially exit relay operators can face legal punishments.

As of 2025, it is estimated that Tor has a total of 7,000 volunteer-run relays worldwide, which include entry, middle, and exit nodes. The number has historically been around 6,000 to 7,000 for several years. However, these numbers do not include nodes called “bridges”, which cannot be publicly seen and used to bypass censorship.

The Creation and Shutdown of Silk Road

Named after a famous Eurasian trade route formed around 130 BCE, Silk Road was first founded by Ross Ulbricht in February 2011. Silk Road was the first major modern darknet marketplace, and it was only accessible through the Tor browser. This, combined with the use of bitcoin as the exchange currency, allowed users to be almost fully anonymous, which led to the large user base of Silk Road with around 100,000 users. While there were safe listings such as health supplements, many people were able to purchase illegal goods, which were mostly drugs. Additionally, they could also browse other listings while also reading reviews. Buyers and sellers had user accounts and reputation scores, just like surface web markets. These factors eventually led to the popular success of the Silk Road. In June 2011, the Gawker blog posted a feature about the Silk Road site, which led to even higher traffic. However, this also attracted law enforcement agencies, such as the DEA (U.S. Drug Enforcement Administration).

An example of a listing in Silk Road (Britannica, 2013)

The first sentence regarding Silk Road happened in June 2012, targeting a drug dealer operating in Silk Road. Later, it was eventually shut down by law enforcement in October 2013, shortly after Ulbricht was arrested. He was charged with a variety of crimes, including criminal enterprise, trafficking drugs, money laundering, and more. The FBI seized around $120 million worth of Bitcoin in total from Silk Road during the shutdown on 2 occasions. In total, Ulbricht was handed 5 sentences, which included two life sentences and 40 years in prison. Later, during the presidential campaign in 2024, Donald Trump stated that he would pardon Ulbricht's life sentence, and on January 21, 2025, after a day he was inaugurated, he fully pardoned Ulbricht.

The takedown of Silk Road marked the first successful international cooperation between countries for targeting darknet marketplaces. After Silk Road's shutdown, law enforcement agencies realized that such operations required global coordination in addition to domestic methods. This

shutdown eventually led to joint operations such as Operation Onymous, and these early coordinated crackdowns set the precedent for UNODC-supported global enforcement campaigns.

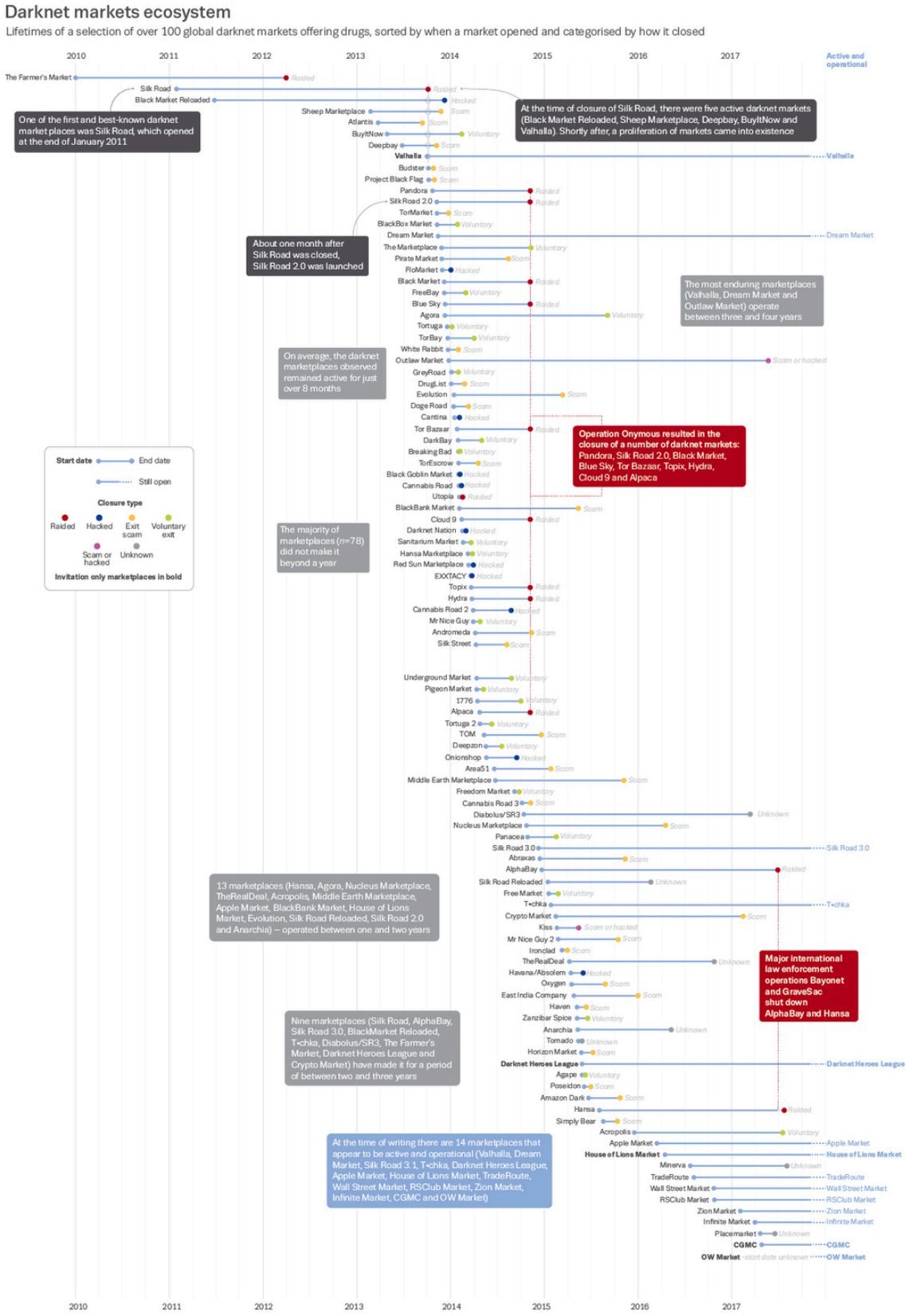
Darknet Marketplaces After Silk Road

Silk Road made a huge impact on large-scale darknet markets. After its fall, similar markets rose in the dark web. One of them was Silk Road 2.0, which came out just a month after Silk Road's shutdown. However, most of them were abruptly shut down. Even Silk Road 2.0 was shut down because of law enforcement and international operations. Despite this, some darknet markets still use the term "Silk Road", while having no connection to the actual Silk Road market, to attract more customers. Other darknet marketplaces also emerged, with one of them being Evolution. It started operating in 2014 and quickly became the new dominant market, and was pretty similar to other darknet marketplaces at that time. Though it had lax rules related to stolen credit card data. However, it suddenly vanished from the marketplace. The creators of Evolution allegedly stole around $12 million worth of users' bitcoin. After Evolution, Agora became the new dominant market. Agora ended in 2015, voluntarily closing the website due to law enforcement pressure and protection of the website against potential cyber attacks. Subsequently, most of the activity was transferred to the AlphaBay website.

AlphaBay & Dream Market Becoming New Dominant Marketplace

After AlphaBay launched in December 2014, it quickly became one of the most popular darknet websites. Soon, its volume surpassed Silk Road, which previously had the record for largest darknet website activity during that time. Some of AlphaBay's features included mandatory PGP (Pretty Good Privacy), two-factor authentication, and use of Monero alongside Bitcoin. Through Operation Bayonet, AlphaBay was closed. Most of the users migrated to Hansa Marketplace, which was also taken down by law enforcement afterwards.

Dream Market became the new dominant marketplace after AlphaBay. Dream Market was active around somewhere in 2019. The reason for the closure of Dream Market is largely unknown and mysterious, with law enforcement and voluntary shutdown being the most plausible reasons. During the era of Dream Market, which is around 2014~2019, other notable large darknet websites include Atlantis, Sheep Marketplace, Black Market Reloaded, and Wall Street Market. Many of these marketplaces were shut down because of exit scams or shutdowns against security and legal threats.



Darknet Markets Ecosystem Overview (EMCDDA and Europol, 2010~2019)

Success of Operation Onymous

Carried out in November 2014, Operation Onymous was a major international law enforcement operation. This was conducted by a joint operation between the US and 16 European Countries. They aimed to shut down platforms in the Tor network that were selling illegal products. Most notably, Silk Road 2.0 was closed, and Blake Brenthall, who was allegedly claimed to be the operator by the FBI, was arrested. Moreover, over 400 .onion sites that were involved in illicit behaviors were seized and taken down. This included other darknet markets, including Black Market, Blue Sky, Tor Bazaar, Topix, Hydra, Cloud 9, and Alpaca. During the operation, a handful of assets were seized by the authorities. One of the most important assets seized was $1 million worth of bitcoin. Other assets included cash, drugs, guns, gold, and silver. Additionally, 17 arrests were made by this operation across several countries, including the USA, Germany, and Ireland.

Operation Onymous's success was able to shatter the long-lasting belief that dark web markets were untouchable by law enforcement during that time, due to the anonymity and high security of the Tor network. Although the exact methods that authorities used were largely disclosed, it showed that rigorous law enforcement could penetrate dark net operations. However, not all darknet marketplaces were shut down through Operation Onymous, with Evolution and Agora being the most popular examples.

Recent Rise of Russian and Short-lived Darknet Marketplaces

Starting from Hydra Marketplace, a massive Russian-language website launched in 2018, there has been a recent rise in darknet marketplaces. Hydra Marketplace handled an estimated value of $5 billion worth of crypto transactions, as well as having around 5 million users. It was seized by a team of US and German law enforcement operations in 2022, while also seizing around $25 billion in Bitcoin. This had a huge impact on darknet platforms in general.

Around 2023 to 2024, after the Hydra Marketplace, there was no 1 dominant marketplace. Instead, there were various small marketplaces that were easier to dodge law enforcement actions, since there were so many of those marketplaces. There was also a large shift from Bitcoin to Monero, as Hydra Marketplace showed that Bitcoin is traceable. The products of it also changed a bit: although sellers still listed various drugs in the marketplace, due to the recent crypto boom, digital products like hacked accounts had a spike.

Recently, Abacus Marketplace grew in popularity in late 2024 to early 2025. They had over 40,000 illicit drug listings, and it grew into a large-scale marketplace in 2025. However, in July 2025, it suspiciously shut down, which was suspected to be an exit scam.

Various Types of Drugs in Darknet Marketplace

A variety of types of drugs are once sold in darknet marketplaces, and some are still being traded currently. Cannabis, synthetic stimulants (amphetamines or MDMA), cocaine, methamphetamine, and synthetic opioids such as Fentanyl are the few examples of the prominent types of drugs. On vendors from Alphabay, the most popular products on sale were stimulants, which includes cocaine and crystal meths. This accounted for 20% of the total sales happening. It was followed by Cannabis, with 18% of total share. It was succeeded by opioids, which includes fentanyl and others like heroin and oxycodone.

Methylenedioxymethamphetamine, or MDMA in short, is another stimulant that is currently sold in illegal ways, although it can also be used in cases like therapeutic purposes for post-traumatic stress order. According to an EU MDMA Market Analysis, it revealed that there was a recent rebound in MDMA seizures and trafficking. In a 2022 darknet study, there were around 8,800 listings on the dark web, with the origins mainly from Germany, Netherlands and France. Interestingly, the price was lower than offline retail inside the dark web than offline transactions.

Illegally manufactured synthetic opioids like Fentanyl is arguably the biggest priority for international cooperation. From October 2022 to the end of September 2023, around 13,000 kilograms of Fentanyl was seized at the United State's border. Considering that only 2 milligram of Fentanyl is deadly, it means that more than 6 billion lethal doses came into the U.S in only 1 year, and this is only for the recorded amount of drugs.

International Laws on Drugs and Darkweb Accessibility

There are currently various laws regarding drugs and the dark web. The International Drug Control Conventions, also known as the "three treaties", which was first established in 1961 and later amended in 1982, aimed to integrate the complex and concurring regulations around the world into one. It aimed to strictly regulate drug use that is unrelated to medical and scientific usage.

Also, UNTOC (UN Convention against Transnational Organized Crime) was ratified in 2003. This aimed to target transnational organized crimes, which includes drugs, as well as strengthening law regulations internally in each nation to act against these crimes.

The Second Additional Protocol to the Budapest Convention, in 2022, enabled faster cross-border data access about computer crime and electronic evidence. By 2025, around 46 countries have signed to this convention. Budapest Convention was the first convention around cybercrime and electronic evidence.

Various Technology and Methods for Tracking Drug Purchase in Darkweb Marketplaces

Currently, a wide range of technologies exist when it comes to tracking down darknet marketplaces and drug purchase. According to a 2023 report from Europol about internet organized crime threat assistant, it mentions Bitcoin tracking. Since wallet activities that use Bitcoin leave a record for each transaction, by further increasing the technological state such as analyzing liquidity pools, cross-chain swaps, and demixing activities, they can more accurately track down Bitcoin usage. However, many recent markets also have a tendency to move towards Monero coin, which is harder to trace because of the structure of the coin being centered on anonymity.

Another method includes training that is being received by organizations for darknet and cryptocurrency training service. For example, during February 2022 in Bangkok, Thailand, UNODC set up a training course in order to counter the trafficking of synthetic drugs. This was a 5-day training, and it was led by UNODC specialists. The participants of this improved their quality of identifying evidence of drug purchase in each stored wallet, as well as understanding varying enforcement methods. As a note, the government of The United States of America funded this course, with the collaboration of UNODC.

In addition to the previously mentioned methods, there is also diverse research on the method of surveillance of darknet websites. According to research that is related to the DNeT project (Drugs and New Technologies), it used partly and fully automated dark web crawling and scraping to gather various data. By getting these kinds of data, organizations are able to monitor the recent trend of online dark web drug marketplace by comparing the share of the type of drug and the marketplace.

Impact of Exit Scams and Shutdowns

Although there are many dark web marketplaces created, they are mostly temporary. There are various ways that those websites can be closed, such as shutdowns, exit scams, volunteer exit, and being hacked. Shutdowns happen when law enforcement agencies manage to identify and seize control of a marketplace, with Silk Road being the most well-known example. Unlike shutdowns, exit scams happen when market operators deliberately disappear, while also taking the user's funds away. This can be done since the user's funds are held in escrow for the payment, as mentioned above.

These have various effects on the use of darknet markets, most of those lowering the use of dark web markets in general as a result. This is due to the fact that when a shutdown or exit scam occurs, large amounts of bitcoins are seized and wiped out by either the government or the operator, which would naturally lead to negative economic consequences. Moreover, it can also worsen the trust of darknet markets, and disrupt the network of illegal trade in general.

Dark Web Usage for Illicit Drug Purchases

Over the past years, drug purchases on the dark web have been fluctuating, with the recent trend rising even with law enforcement. According to a statistical report in 2021, over $2.1 billion was generated in darknet marketplaces in cryptocurrency. More than $1.8 billion of it was from illicit drug purchases, and the remaining $300 million was mostly from fraud markets. Compared to $1.4 billion in 2019 and $1.8 billion in 2020, the use of darknet marketplaces has grown, but dropped almost in half during 2022, with the impact of the dismantlement of Hydra Market, a Russian darknet website. Nevertheless, the darknet market recovered in value, and despite various law enforcement actions, it reached approximately $1.7 billion in 2024. It is also worthwhile to note that more than 90% of total activity was from Russian marketplaces in Bitcoin and TRON, due to Russian law enforcement being a lower threat in comparison with other nations, and wide availability of drugs from China. Meanwhile, European darknet websites were faced with sustained law enforcement actions and exit scams.

National Dark Web Usage

Considering the userbase of Tor, which is the most popularly used darknet website domain, as of 2025, the country with the most dark web users is the United States. It has around 21.4% of Tor user browsers each day on average. This is followed by Germany, which has an estimated 12.9% of total Tor users every day. It is succeeded by Finland, which has a daily user base of 5.2%. Other

countries with a high number of Tor accounts include India (3.9%), Russia (3.5%), France (3.4%), Indonesia (3.0%), the Netherlands (2.7%) and the UK (2.6%).

Possible Solutions

Most of the nation's consensus is that although the dark web can be used for legal purposes, using dark web marketplaces for illegal purposes in general should be penalized. However, the extent to which punishment will be given currently differs in each nation. This creates a problem when the crime is across several countries, which is currently happening more with globalization. Additionally, more development of tools for tracking down darknet marketplaces is also crucial for operations and shutting down marketplaces, as well as education programs for the dangers of darknet and drug use, due to the fact that it is almost impossible to track down all the darknet marketplaces that are operating illicitly.

Increasing Global Cooperation for Law Enforcement

A highly coordinated transnational law enforcement network, backed up by organizations like Interpol and Europol and initiatives such as the J-CODE and Eurojust, enables nations to take down darknet marketplaces more efficiently and effectively. DisrupTor, SpecTor, Dark HunTor, and Archetyp Market's shutdown are shown as successful examples of globally coordinated law enforcement attacks. Some of the key mechanisms that are used for global cooperation include MLATs (Mutual Legal Assistance Treaties), extradition agreements, coordinated intelligence exchange platforms, and joint cyber-task forces.

Standardised Legal Punishments

In various nations, there is a lot of divergence among specific sentences related to dark web marketplaces. Without consistency in criminalized conduct and sentencing thresholds, criminals might have a chance to exploit legal loopholes. For example, updating EU framework decisions (for EU nations), ratifying treaties that are related to the dark web, can be some of the solutions. Uniform punitive frameworks could be able to deter cross-national drug dealers and strengthen cooperation.

Funding for the Development of Darkweb Monitoring Tools

Continuous funding to support the creation and deployment of advanced investigative technologies is crucial for dealing with dark web marketplaces that are evolving to not get caught. If there are new agencies with the objective of combating the dark web, they would need the specialized

tools for constant adoption with the new darknet techniques. Similarly, the UNODC is currently providing cybercrime training across several nations, which is to reinforce member states' technical investigations.

For example, there are currently various Artificial Intelligence developed for dark web tracking. One of them is StealthMole, which is a Singapore-based AI-powered dark web monitoring startup with an R&D office in South Korea that is focused on the monitorization of cyber threats in the dark web and detection of cybercrime. It announced that it has raised $7 million for their startup. With support from the government, these kinds of startups would be able to more effectively cover the darknet website.

Increasing Public Awareness

To reduce the use of the dark market, not only is law enforcement needed, but demand suppression is also very paramount. Organizations such as UNODC and SCO report that most darknet transactions involve synthetic drugs, and younger internet users are excessively exposed to drug marketplaces. Additionally, public education campaigns targeting younger generations and communities raise awareness of illicit drugs and the obscure hazards of darknet marketplaces. International organizations should promote curricula and awareness campaigns to reduce drug demand.

Major Parties Involved

Russian Federation

With various Russian-language-based platforms conducting various online illicit drug activities, Russia has now become a dominant force in the darknet economy. These kinds of activities were also seen in the early days of darknet marketplaces, after the Silk Road was taken down. RAMP (Russian Anonymous Marketplace) was one of the earliest sustained darknet websites, which also lasted longer than Silk Road and Silk Road 2.0 combined due to its website structure, and also being a Russian-based model, which made law enforcement difficult. By 2022, Russian-language darknet markets accounted for around 80% of the global sum of $1.49 billion for illicit drug purchase. One of its reasons for the success was due to its innovative model called “Dead Drops” that was done around the city.

After Hydra Marketplace, which was also a Russian-language-based darknet marketplace with over $5 billion in illicit crypto transactions, was taken down, it made various other successors of the website emerged. Kraken, Solaris, RuTor, WayAway, Mega, and others engaged in various activities like aggressive marketing to get a share of the remaining users of Hydra Marketplace. Most of these websites were unlike traditional Tor-based websites. Instead, they were leaning towards instant and agile messaging and transactions.

Law enforcement in Russia domestically relies on GUKON (Main Directorate for Drugs Control), with strict surveillance laws like the Yarovaya laws. However, disrupting the major darknet websites like Hydra Marketplace needs international law enforcement cooperation, which can be seen when Germany was able to take down Hydra with the cooperation of Russia.

The United States of America

Although the United States of America is one of the countries with high usage of the dark web, they also play a leading role in global efforts to prevent darknet marketplaces’ illicit drug trafficking. J-CODE (Joint Criminal Opioid and Darknet Enforcement), which is a task force that was established by 2018, is a permanent multi-agency with the role of uniting various agencies and international organizations to combat drugs inside of dark web, including the DOJ (U.S. Department

of Justice), FBI (Federal Bureau of Investigation), DEA (Drug Enforcement Administration), and more.

Additionally, the United States has also spearheaded various operations that aimed at darknet markets, such as Operation DisrupTor, Dark HunTor, and SpecTor. There were also legislative efforts, such as the Dark Web Interdiction Act of 2025. While these operations have resulted in significant amounts of funds being seized dozens of times around the world, there are still some darknet websites roaming around the darknet in the USA.

People's Republic of China

China applies a rigorous and multifaceted strategy to counter the globally varying dark web marketplaces. It emphasizes harsh penalties and wide public education campaigns to foster strong anti-drug attitudes among its population. It has specialized agencies like the Ministry of Public Security's Drug Control and Online Safety bureaus, and extensive data surveillance via its Dynamic Control System, as well as various national education campaigns. Internationally, they collaborate with global partners to control through with countries such as Mexico and also engage with U.S. law enforcement. Despite these types of legal measures, challenges remain in balancing privacy rights and addressing human rights concerns around mass surveillance systems in China.

Federal Republic of Germany

Germany has become a key player in disrupting the darknet drug trade through enforcement operations, strong institutional capacity, and international collaboration. Key agencies such as the BKA (Federal Criminal Police Office) led major takedowns such as the seizure of Hydra Marketplace and DarkMarket. Germany also works with Europol and Eurojust for multinational initiatives such as Operation Dark HunTor and SpecTor. Together, these strategies demonstrate Germany's commitment to dismantling major crypto-enabled drug marketplaces.

Republic of Finland

Domestic studies in Finland show that nearly half of all drug purchasers there use darknet platforms. To combat these, Finland operates a combination of proactive cyber surveillance and targeted enforcement, both physical and digital. Finland also cooperates internationally, such as

Poland, Sweden, and Europol. However, some authorities also state that the limited digital resources at the regional level are an obstacle to deeper darknet investigations.

Republic of India

In June 2023, the NCB (Narcotics Control Bureau), India's agency fighting against drug trafficking, dismantled India's largest darknet-based LSD organization, which was named after a type of drug and also called the "Zambada cartel". This was marked as India's biggest single seizure. It was also an international cooperation among various states including the US, the UK, Poland, South Africa, and others. To support investigations, India established task forces, upgraded cybercrime protocols, and systems such as I4C, the Cyber Crime Reporting Portal, and data-sharing networks over their provinces. Moreover, UNODC, with support from the US State Department, conducted a five-day training in New Delhi for Indian law enforcement. In general, India is putting effort toward a more technically proficient and internationally coordinated approach to disrupt darknet drug supply chains.

Kingdom of the Netherlands

The Netherlands is the foremost on combating darknet drug trafficking in various cooperating ways. In a joint effort with several countries, the Dutch police took control of Hansa Market, which was a marketplace that attracted many users after Alphabay's closure. Instead of normally taking down the marketplace instantly, they "operated" the market for 27 days. This allowed the Netherlands to gain data on approximately 420,000 users. Also, one of the 'Bohemia/Cannabia' darknet marketplace operators, a marketplace that had over 12 million euros in monthly transactions, was taken down in 2024 by Netherlands authorities.

Dominion of Canada

Various operations in Canada such as Hackstone, Ontario's Project Bionic and Golden successfully dismantled various darknet marketplaces. Canada's Border Plan and Directive on Transnational Crime also reinforce intelligence coordination across CBSA, RCMP, CSE, and Public Safety Canada. Furthermore, Canada aims to extend their efforts internationally, by having cross-border forums like CBCF, and sharing information with the U.S in order to strengthen global cooperation, preventing darknet drug trafficking.

Timeline Of Events

Date	Description of Event
Development of Onion routing, 1990s	Syverson, Dingledine, and Mathewson, who were employees in the U.S. Naval Research Laboratory, developed the core principles of Tor.
Launch of Tor (The Onion Routing) Project, September 2002	To support anonymous connections online,the Tor Project was launched by the U.S. Naval Research Lab.
Tor Network under Free License, 2004	After Tor was freely licensed, the EFF (Electronic Frontier Foundation) started funding Dingledine and Mathewson to continue developing the Tor network.
Creation of The Tor Project, 2006	Dingledine, Mathewson, and five other people founded The Tor Project, which was a non-profit organization that maintained Tor.
First usage of term "Dark Web", 2009	The term Dark Web first appeared in a newspaper article, and it described illicit activities happening in Tor network during that time.
Creation of Silk Road, February 2011	Ross Ulbricht founded Silk Road, which is considered to be the dark web's first black market.
Arrest of Ross Ulbricht, October 2013	The U.S. The FBI (Federal Bureau of Investigation) arrested Ulbricht and took down the Silk Road. However, imitators of Silk Road arose, with Silk Road 2.0 being the most popular.
Operation Onymous and Agora Market being the new dominant darknet market, November 2014	After dozens of darknet marketplaces, including Silk Road 2.0, was taken down by Operation Onymous, Agora Market became the new dominant market.
Agora's Shutdown and Dream Market's Rise, 2015	Agora Market's voluntary shutdown after law enforcement pressure caused the Dream Market to gain more popularity.

Operation Bayonet and the seizure of AlphaBay, July 2017	AlphaBay, which is known to be founded by a Canadian, was the largest darknet market during that time, but it was seized by Operation Bayonet.
Shutdown of Dream Market, March 2019	Although Dream Market was the dominant market during this time, while also lasting around 6 years, which is a very long duration for darknet marketplaces in comparison, several DDoS attacks and law enforcement pressure made it shutdown.
Operation DisrupTor, September 2020	$6.5 Million worth of Cash and Digital currency and 500kg of drugs were seized, and various agencies internationally cooperated, some of them being the FBI, USPIS (United States Postal Inspection Service), HSI (Homeland Security Investigations), and Europol.
Operation Dark HunTor, January 2021	$31 million in cash and crypto, as well as 234kg of drugs and 45 firearms, were seized. Nations such as Australia, Bulgaria, France, Germany, Italy, the Netherlands, Switzerland, the UK, and the US led this, with Europol and Eurojust's assistance. It also took down DarkMarket, the biggest Darknet Marketplace at that time.
Shutdown of Hydra Market, April 2022	The largest Russian-language market, Hydra Market, was shut down by German authorities and U.S. law enforcement.
Rise in Russian Darknet Markets, 2023	Many Russian darknet markets, including Mega, OMG!, and BlackSprut, filled the gaps of Hydra Market.
Abacus Market's Suspected Exit Scam, July 2025	The current largest Western bitcoin-supporting darknet marketplace, Abacus Market, shut down its website which is suspected to be an exit scam.

UN Involvement, Resolutions, Treaties, and Events

- INCB (International Narcotics Control Board)

INCB is the UN's independent, semi-judicial body that monitors how countries adhere to the three major drug control treaties. In its 2023 Annual Report, INCB highlights how drug traffickers exploit not just darknet marketplaces, but also deep web and surface web platforms such as social media, postal, and e-commerce services. It warns that encryption, anonymous browsing, and cryptocurrency usage present enforcement challenges, and stresses the need for both public and private cooperation.

- Darknet Cybercrime Threats to Southeast Asia

This UNODC's regional report on Southeast Asia was written in 2020 and originally published in 2021. It offers an extensive analysis with the primary focus on encrypted drug sales. One of the key data points that was recorded in this report is that approximately 68% of the nearly 139,000 items listed on four major darknet markets were drug-related. The report also warns of limited data, weak enforcement frameworks, and legal gaps in regional cybercrime statutes in Southeast Asia.

- CNDs (Commission on Narcotic Drugs), which are UN's central policy body on drugs, focus on regularly featuring briefings and submissions from INCB and UNODC on darknet drug trade trends. For example, INCB contributions to the 67th CND, consists of chapters with the primary focus of darknet misuse and online platforms. These calls for immediate action such as enhancing international and cross-sector cooperation to counter darknet marketplaces.

Bibliography

Charlton, Alistair. “Operation Onymous: Six Britons Arrested as Police Bust 400 Drug Dealing Dark Websites.” *International Business Times*, November 2014, https://www.ibtimes.co.uk/operation-onymous-six-britons-arrested-police-bust-400-drug-dealing-dark-web-sites-1473713.

“CRYPTOCURRENCY | English meaning - Cambridge Dictionary.” *Cambridge Dictionary*, https://dictionary.cambridge.org/dictionary/english/cryptocurrency.

“Cybersecurity Spotlight - The Surface Web, Dark Web, and Deep Web.” *CIS Center for Internet Security*, 2019, https://www.cisecurity.org/insights/spotlight/cybersecurity-spotlight-the-surface-web-dark-web-and-deep-web.

“Darknet Cybercrime Threats to Southeast Asia.” *United Nations Office on Drugs and Crime*, Jeremy Douglas and Neil J. Walsh, 2020, https://www.unodc.org/roseap/uploads/archive/documents/darknet/index.html.

“Darknet Markets Ecosystem — Information is Beautiful Awards.” *Information is Beautiful Awards*, 2019, https://www.informationisbeautifulawards.com/showcase/3159-darknet-markets-ecosystem.

EUROJUST. “Second Additional Protocol to the Budapest Convention on Cybercrime and Cross-Border Access to Electronic Evidence.” *European Union Agency for Criminal Justice Cooperation*, 27 July 2022, https://www.eurojust.europa.eu/publication/second-additional-protocol-budapest-convention-cybercrime-and-cross-border-access.

“Everything You Should Know About the Dark Web.” *Tulane School Of Professional Advancement*, https://sopa.tulane.edu/blog/everything-you-should-know-about-dark-web.

Freist, Roland. “What is the Tor network? The anonymous internet, explained.” *PCWorld*, October 2024, https://www.pcworld.com/article/2476461/what-is-the-tor-network.html.

Graham, CLULEY. “Dark web drug market Evolution vanishes off the net, taking millions of dollars with it.” *Bitdefender*, 19 March 2015, https://www.bitdefender.com/en-us/blog/hotforsecurity/dark-web-drug-market-evolution-vanishes-off-the-net-taking-millions-of-dollars-with-it.

Greif, Björn. “Tor network: definition and functionality.” *Myra Security*, https://www.myrasecurity.com/en/knowledge-hub/tor-network/.

INCB. “The role of the Internet in drug trafficking and drug use is highlighted in the International Narcotics Control Board Annual Report.” *International Narcotics Control Board*, INCB, 5 March 2024, https://www.incb.org/incb/en/news/press-releases/2024/the-role-of-the-internet-in-drug-trafficking-and-drug-use-is-highlighted-in-the-international-narcotics-control-board-annual-report.html.

“Internet Organised Crime Threat Assessment (IOCTA) 2023.” *Europol*, Europol, 2023, https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202023%20-%20EN.pdf.

Nicola Man, Yan Yang, Vandit Sadaphale, Qingyuan Linghu, Raimondo Bruno, Monica J. Barratt, Rachel Sutherland and Amy Peacock. “Trends in the availability and types of drugs sold on the internet via cryptomarkets.” *Drugs and New Technologies*, September 2023, https://archive-ndarc.med.unsw.edu.au/sites/default/files/ndarc/resources/Cryptomarket%20methods_Sep%202023.pdf.

Pangarkar, Tajammul. “Dark Web Statistics and Facts (2025).” *Market.us Scoop*, 2025, https://scoop.market.us/dark-web-statistics/.

Rasure, Erika. “What Was the Silk Road Online? History and Closure by the FBI.” *Investopedia*, 2025, https://www.investopedia.com/terms/s/silk-road.asp.

Rosenston, Michael. “How Escrow Protects Parties in Financial Transactions.” *Investopedia*, October 2024, https://www.investopedia.com/terms/e/escrow.asp.

“39 Must-Know Dark Web Statistics for 2025 | Panda.” *Panda Security*, 5 May 2025, https://www.pandasecurity.com/en/mediacenter/dark-web-statistics/.

"Tor and Beyond: Key Developments in the History of the Darknet." *DARKOWL*, July 2023, https://www.darkowl.com/blog-content/interactive-timeline-tor-and-beyond-key-developments-in-the-history-of-the-darknet/.

Toulas, Bill. "Abacus dark web drug market goes offline in suspected exit scam." *Bleeping Computer*, 15 July 2025, https://www.bleepingcomputer.com/news/security/abacus-dark-web-drug-market-goes-offline-in-suspected-exit-scam/.

TRM. "Eight Months After Hydra Shutdown, New Russian-language Darknet Markets Are Filling the Void." *TRM*, 5 December 2022, https://www.trmlabs.com/resources/blog/eight-months-after-the-hydra-shutdown-new-russian-language-darknet-markets-fill-the-void.

UNODC. "Darknet Cybercrime Threats to South East Asia." *Sharing Electronic Resources and Laws on Crime*, UNODC, 2020, https://sherloc.unodc.org/cld/bibliography/2020/darknet_cybercrime_threats_to_south_east_asia.html.

UNODC. "The International Drug Control Conventions." UNODC, 1961, https://www.unodc.org/documents/commissions/CND/Int_Drug_Control_Conventions/Ebook/The_International_Drug_Control_Conventions_E.pdf.

UNODC. "International Narcotics Control Board Contribution to the Commission on Narcotic Drugs 2024 mid-term review of progress in imple." *UNODC*, 15 February 2024, https://www.unodc.org/documents/commissions/CND/CND_Sessions/CND_67/Stakeholder_Contributions/All_Challenges/INCB_contribution_-all.pdf.

UNODC. "United Nations Convention against Transnational Organized Crime." *United Nations Office on Drugs and Crime*, 29 September 2003, https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html.

"UNODC delivered the cryptocurrencies and darknet investigations training course." *UNODC Regional Office for Southeast Asia and the Pacific*, 25 February 2022, https://www.unodc.org/roseap/en/2022/02/cryptocurrencies-darknet-investigations/story.html.

Volle, Adam. “Dark web | Definition, The Onion Router, History, & Examples.” *Britannica*, 27 June 2025, https://www.britannica.com/technology/dark-web.

“What is Dark Web? How It Works & Why It's So Dangerous.” *EC-Council University*, Augest 2024, https://www.eccu.edu/blog/the-dark-web-and-its-dangers/.

“What is Monero (XMR)?” *Monero*, https://www.getmonero.org/get-started/what-is-monero/.

“With Criminal Groups Using Sophisticated Technologies to Ply Their Wares, Third Committee Stresses Urgent Need to Collectively Combat Transnational Crime | Meetings Coverage and Press Releases.” *Meetings Coverage and Press Releases*, 2 October 2023, https://press.un.org/en/2023/gashc4374.doc.htm.