Committee: UNODC
Topic: The growth of online black markets on the dark web
Chair: Julia Paola Garcia Sánchez
Moderator: Juan Daniel Sánchez Zatarain

Overview of the Problem

The United Nations Office on Drugs and Crime (UNODC) is responsible for tackling the worldwide drug problem currently happening, fighting organized crime that operates through the dark web, preventing and countering terrorism, and addressing many more situations connected to the creation of illegal activities such as drug dealing. The growth of dark web marketplaces has accelerated substantially over the past fifteen years as digital infrastructure expanded. This leads to online black markets continuing to operate with even more effective facilities and in several new ways, so they cannot be tracked easily. In addition, they fuel illegal large-scale cybercrimes and operate entirely outside the reach of traditional legal frameworks. (UNODC, 2026)

International organizations such as the European Union Agency for Law Enforcement Cooperation (EUROPOL), the United Nations Office on Drugs and Crime (UNODC), the Five Eyes Law Enforcement Group (FELEG), the FBI & DEA (United States of America), and the ICE Homeland Security Investigations address this problem by assisting several countries in need of support to fight these situations that could lead to terrorist attacks or organized crime consequences. Nevertheless, the countries that help enforce this issue the most are the United States of America (USA), the United Kingdom (UK), Germany (GER), the Netherlands, Australia, Canada, France, Belgium, Finland, Romania, Slovakia, Japan, South Korea, the United Arab Emirates (UAE), and Saudi Arabia.

Several major issues make it difficult for the UNODC to address this situation. The rapid transformation of underground technology outpaces the UNODC's

technical assistance guidelines. In addition, the lack of technological infrastructure in several nations makes it harder for any organization (especially the UNODC) to track any case of black market “trade” on the dark web and find a solution to assist them properly.

Delegates will share the committee members' perspectives on the issue and then talk about how to strike a balance between keeping the users' privacy intact and addressing the issue of fighting black market growth on the dark web. Additionally, delegates will talk about how to guarantee equitable responsibility distribution between the several present delegations and rule compliance. The committee will also investigate new instruments, organizations, or treaties that can help enhance the addressing of these situations in the future. Among the crucial subjects of discussion, the debate will also be centered on enhancing international cooperation, increasing the ways to address this issue, and identifying long-term solutions.

Introduction

The dark web is a hidden part of the internet that uses special networks such as Tor; it uses encryption and indirect routing for greater anonymity. The dark web is unlike the surface web, which is composed of websites that are easy to find with traditional search engines. The dark web needs special software or settings to be accessed. It has also become a space for illegal activities, including the operation of online black markets. But it also serves legitimate purposes, such as protecting journalists, whistleblowers, and people living under censorship.

Online black markets are venues where individuals and criminal organizations buy and sell illegal products, such as stolen personal information, financial information, malware, and access to hacked computers. These markets function a lot like legitimate e-commerce sites with product listings, seller ratings, customer reviews, and cryptocurrency payments. But their anonymity makes it

difficult to vet sellers, identify buyers, and hold those responsible for criminal activity accountable. These new markets therefore present new challenges to governments, law enforcement agencies, and cybersecurity professionals around the globe.

The growth of online black markets is a major international concern because of its potential consequences for individuals, businesses, and national security. The theft of login credentials and financial information can result in identity theft and economic losses. Services for malware and ransomware enable criminals to carry out increasingly sophisticated cyberattacks. Compounding the problem, criminal marketplaces can re-emerge after authorities shut down existing platforms.

The solution to this issue will depend on international cooperation, improved cybersecurity measures, efficient law enforcement, and increased information sharing across the law enforcement, private, and research sectors. Cybersecurity practitioners watch open-source threat intelligence and investigate data breach reports, while nations can cooperate to improve law enforcement activities regarding cybercrime. Proposals for new initiatives must also respect valid privacy rights and ensure that all dark web-related activities are not painted as illegal, as anonymity can also serve important purposes.

Delegates will investigate the elements promoting the rise of online black markets on the dark web via the committee, as well as analyze the issues affecting efforts to unmask these networks. They will discuss the effects of these actors on the economy, technology, and law. Delegates will evaluate not only the efforts made at the international level but also the disadvantages of presently used methods to learn solutions that would take into consideration cybersecurity and public safety issues along with the importance of privacy and international cooperation.

Historical Background

The first darknet markets came into existence in about 2010, which employed encrypted networks and communication systems to make transactions less traceable. By January 2011, Silk Road became one of the earliest markets to become popular by using the Tor network and bitcoins as part of the illegal sales of its products. Its reputation demonstrated that the internet can be a rewarding business for both buyers and sellers. (ESET blog, 2025)

In October 2013, the FBI seized Silk Road and arrested its administrator, permanently shuttering the original platform before copycat networks emerged. Nonetheless, the online platform still continues to function. Silk Road 2.0 was launched just a month later together with many more markets. In November 2014, Operation Onymous was carried out in order to undermine a number of darknet markets. All these facts illustrate not only an increasing scale of the issue but also the difficulties of preventing new platforms from being created. (Kosinski, n.d.)

AlphaBay is a darknet marketplace that started back in December of 2014. Soon enough, it became one of the biggest darknet marketplaces selling illegal goods, stolen data, and other cybercrime products. The success of AlphaBay proves that the darknet market expands beyond the drug market and into other forms of electronic crime. In July of the year of 2017, an international operation was conducted that shut down both AlphaBay and Hansa Marketplace. It’s clear that international collaboration is essential for investigating cybercrime. (United Nations Office on Drugs and Crime, n.d.)

While some marketplaces voluntarily shut down and others suffered cyberattacks, authorities also targeted several major markets in 2019, including

Dream Market, which ceased operations after years of being in business. (EUROPOL, 2019)

However, it can be stated that police raids shed light on weaknesses of the darknet that contributed to the rise of different black platforms.

In 2020, law enforcement authorities seized more than 1 billion USD worth of cryptocurrency tied to Silk Road illicit proceeds, meaning that financial investigations are still very important in fighting crimes in these markets. (Department of Justice, 2020)

It is difficult to have accurate estimates of the size of the online black market due to the ephemeral character of most such platforms. According to research conducted by the European Monitoring Centre for Drugs and Drug Addiction, many digital platforms last for only a short time period or close down for various reasons. Yet, the issue of cybercrime trade, including sales of stolen goods and malicious software used for digital offensives, remains an important security issue. (European Union Agency for Criminal Justice Cooperation, 2019)

In the case of online marketplaces dealing with illicit goods, just as they rise due to increased technological anonymity and global connectedness, enforcement agencies can disrupt or shut down individual platforms, but the entire system cannot be wiped out. Consequently, the necessity of activating international cooperation, cybersecurity measures, financial investigations, and action plans that would address the causes of operation of such markets cannot be ignored. (Marchini, 2025)

The Situation Today

While some regions rely on well-established companies or corporations for basic daily survival or as a way to gain profit to have what populations call a “normal life”, other regions are dominated by highly influential and sophisticated criminal syndicates dealing in high-value digital or financial contraband. Nevertheless, there are nations, regions, or states whose Gross Domestic Product (GDP) encompasses both corporate earnings and individual income from productive economic activity and the consequences of illegal trades. Nations such as Mexico, Russia, Nigeria, and Indonesia are examples of countries facing these parallel economies. (Aqrawi, M., Bazilian, D., & Widdershoven, n.d.)

These are the percentages of GDP coming from the black market by region:

REGION	Percentage of its economy coming from black markets
North America	5.0%
Western Europe	6.6%
Middle East	8.2%
Eastern Europe	11.8%
Western and Central Asia	16.2%
Southeast Asia and Pacific	16.7%
Central America and Caribbean	17.5%
South America	20.0%
Northern Africa	24.1%
Southern Africa	25.9%
Southern Asia	27.2%

Western Africa	31.5%
Middle Africa	33.8%
Eastern Africa	41.6%
WORLD	11.8%

The oversight of growing black markets through the dark web has led to the creation of several internal issues within this specific situation. One example is the creation of micro-smuggling through common delivery packages. Rather than moving masses of illicit products, such as pharmaceuticals or drugs, organized crime organizations have implanted micro “samples” into several packages so the authorities do not suspect anything. This leads to the discreet smuggling of massive groups of illicit substances hidden in tiny places among common deliveries. (Besta, 2025)

Examples:
Several organized crime organizations (mostly Mexican Cartels) have transported illicit substances through cargo ships and parcel-delivery aircraft so authorities do not have a track of what these organizations send to foreign countries. According to recent drug enforcement findings, organized crime groups increasingly utilize encrypted digital platforms and dark web storefronts to market synthetic narcotics due to the fact that moving drugs through this method has proven more effective for the organization, and it hides them from local and international authorities. (Besta, 2025)

Key Stakeholders and Their Positions

There are several stakeholders that are concerned with the problem of the increasing online black markets on the dark web. Various governments, international organizations, non-profit organizations, businesses, and ordinary people are involved in the issue. While law enforcement and government organizations concentrate on fighting crime, businesses are more concerned with cybersecurity, and non-profit organizations work to guarantee privacy and respect rights. To achieve an effective international strategy, it is crucial to know what interests and positions these actors have. (Sherloc, n.d.)

The policy of the United States of America (USA) centers on combating cybercrime, money laundering, and illegal e-commerce. They support the functions of law enforcement agencies in investigations, the tracking of cryptocurrencies, and the cooperation of the agencies internationally in dealing with flourishing criminal markets. European countries focus on transnational organized crime, cyberattacks, and online scams. Through Europol, they cooperate in information sharing and investigation coordination. Mexico prioritizes dismantling cross-border digital financial trails used by transnational cartels to purchase synthetic drug precursors on encrypted platforms. Some international organizations like INTERPOL help countries with information exchange and criminal investigation. (United Nations Peace and Security, n.d.)

The United Nations Office on Drugs and Crime UNODC provides help to governments to stop crime, create a perfect criminal justice system, and increase transparency on an international level. INTERPOL makes the process of information sharing, investigation of cybercrimes, and international crime investigations easier. EUROPOL specializes in assisting European countries in investigations related to online crime, fraud, and markets. EUROPOL puts stress on cooperation, as criminal groups are able to change the mode of their actions quite fast.

The Electronic Frontier Foundation (EFF) advocates for digital privacy rights and defends the legal use of encryption technologies. In the digital realm, it champions encryption and freedom of speech. They contend that while combating cyber-related crimes, the right to privacy must not be infringed. Researchers from the Tor Project have designed a number of innovations that ensure people's anonymity online. Despite the fact that criminal representatives may use the aforementioned technologies, they certainly help journalists, activists, and ordinary citizens in totalitarian regimes by providing possibilities for private communication. (Tor, n.d.)

Businesses such as Microsoft strive to spot and neutralize cyber dangers and stop the functioning of criminal syndicates. In addition, the underground economy constitutes a risk for commercial entities by putting them at risk of suffering from crime involving stolen information, viruses, and other kinds of cyber attacks. Banks and some financial organizations are involved in stopping financial fraud, detecting money laundering, and ensuring protection of customers' financial data. Companies working as internet service providers must make every effort to protect their systems from abuse while safeguarding the access and privacy of the clients.

Identity theft, monetary fraud, and distribution of private data through online criminal circles are some of the dangers people face nowadays. Groups such as small businesses and communities may not be able to sufficiently address the problem of cyberattacks. Affordable solutions should be sought by authorities, supported by carrying out a campaign to raise awareness about the problem. However, some activists and journalists use anonymity tools to be able to protect their identities. Their concerns signify that it is necessary to strike the balance between fighting cybercrime and protecting privacy against censorship.

Though all stakeholders are likely to be interested in minimizing cybercrime, their attitudes towards this matter can diverge. Thus, nations and law enforcement

agencies would probably have their attention focused on investigations and eliminating criminals; international agencies would focus on cooperation, businesses would care about the security of business information, and human rights organizations would advocate for privacy and freedom of speech. An appropriate way to address the issue should be a combination of law enforcement measures, information sharing, crime prevention programs, and support for victims. (United Nations Office on Drugs and Crime, n.d.)

Past Attempts and Existing Frameworks

The UN General Assembly adopted resolution 74/247, creating an ad hoc intergovernmental committee to draft a comprehensive international convention on countering cybercrime. While the rest of the resolutions related to this topic address the issue in maritime environments, this one is specific in assisting with the adversity in a digital setting. In addition, the UN established the UN Cybercrime treaty (finalized in late 2024/ adopted 2025). This treaty specified a framework for countries to rapidly share digital evidence and intercept encrypted communication networks across borders to combat online drug trafficking marketplaces. (Marchini, 2025)

Throughout history, the UN and multiple international organizations and governments have initiated numerous projects. The Operational Chemical Branch (INCB), for example, aims on tracking the online sale and shipment of several chemical substances, pharmaceuticals, drugs, etc. Additionally, INTERPOL's Operation Garuda assists in tracking coordinated international mail shipments to verify that every object that is being shipped is secure and to ensure not only the customers' safety, but also the deliverer's, company's, etc. (INTERPOL, 2022)

Talking about regional programs, the European Union's Digital Services Act (DSA) and the United States STOP Act share various similarities in how the two acts fight or address this issue.

They both shift the burden of proof onto the middleman. Meaning both institutions stop “pursuing” the criminal, but also the intermediary network that is assisting the organized crime doing the action. They also count on advanced data systems that can track the felon and where their actions are going to have an impact.
But which actions did work for the delegations?
Coordinated stings between law enforcement and tech giants have successfully shuttered most of the trails made by cartels' e-commerce proceeds in the black market. Also, forcing international packages to carry digital manifests allows the authorities to ensure there is no illicit object within the deliveries.
On the other hand, different solutions haven’t had that much of an effective response to this issue. The hydra effect is a counterintuitive phenomenon where actions taken to reduce or eliminate a problem inadvertently cause it to multiply or grow. It is given when the authorities track and shut down the cartels’ e-commerce systems, but a built-in AI within their programs, mirrors their whole server for them to keep producing several illegal trades.
Member states continue to debate which technical tools and monitoring frameworks are more effective. Even though local authorities could have several systems tracking these situations, an AI-assisted server for the experts would be as effective as having a whole team trying to solve a case.
AI could track cases in terms of hours, if not minutes.

Challenges and Complications

The establishment of black markets on the Internet has caused a lot of problems for governments and international institutions that want to control them. Because online black markets operate across national boundaries, countries must cooperate and reconcile differences in laws, resources, and IT security measures.

Conflicting national data privacy frameworks and cumbersome Mutual Legal Assistance Treaties (MLATs) frequently delay international digital evidence sharing. Furthermore, many countries lack the necessary funds, trained

personnel, and modern technology for investigating anything that happens online.

The role of technology cannot be ignored in the matter. Such technologies as encryption and anonymity make it difficult to trace criminals and recover the needed digital evidence. In addition, variations regarding regulations that are exercised within individual countries and specific mechanisms of information sharing may extend the duration of investigations or complicate international prosecution processes.

Moreover, issues including privacy, free speech, and access to information differ from one country to another. Therefore, international responses to crime must strike a balance between combating crime and protecting the rights of citizens.

This basically proves the significance of cooperating internationally, having better cybersecurity measures, establishing similar legal practices across countries, and accepting human rights in order to fight online crime efficiently.

The Committee's Role and Powers

Established in 1997 as a specialized body within the United Nations system, the United Nations Office on Drugs and Crime (UNODC) works to fight organized crime among nations, ensure its population’s safety, and prevent any trade of illicit substances. The UNODC committee in the Model UN replicates this practical function by modeling how global communities handle the black market crisis through dialogue, debates, and discussions.

The committee’s authority is based in large part on advocacy, coordination, and respect between delegations rather than enforcement. UNODC’s goal is to arrive at a conclusion each delegate accepts, and this will be achieved by discussing the situation given by the committee and questioning each delegation’s perspective.

Delegates in the Model UN simulate this procedure by creating non-binding resolutions that specify frameworks, funding plans, and proper policies for each delegation

Each delegate will be required to adhere to the parliamentary procedure established by the Model United Nations. The UNODC exercises authority through the UN Convention against Transnational Organized Crime (UNTOC). It exercises authority through the UN Convention against Transnational Organized Crime by delivering specialized technical training and legislative assistance to member states. It is expected that the delegates uphold moral principles and authentically represent the policies established by the delegate's nation.

The UNODC committee enables any delegate to propose human solutions to address this situation as fast as possible so a resolution can be passed.

Guiding Questions for Debate

1. How can countries work together to close online black markets?
2. Should the government be able to limit the use of anonymity tools while protecting legitimate users?
3. How can international organisations help countries with little financial resources and technology to tackle online black markets?
4. What actions can be taken to ensure criminal marketplaces don't reform?
5. How could governments and companies work together to share their information about cybercrime but also ensure the users' privacy?
6. Should tech companies be liable for the illegal activities that occur within their platforms?
7. How can countries improve their international laws to make sure crime involving digital evidence that is stored internationally can be investigated?

8. What role should cryptocurrencies and also financial institutions play to prevent illegal transactions without restricting their legitimate financial activities?
9. What actions can be taken to reduce the demand for illegal products and stolen data?
10. What would be the most effective long-term strategy to reduce online black markets internationally?

Conclusion and Call to Action

The expansion of online black market activity within the dark web represents a pressing international challenge. It is a significant global issue. It poses threats to our cybersecurity, financial security, privacy, and safety. Black markets allow the illicit trade of stolen data, illegal products, and cybercrime services. This threatens individuals, businesses, and governments globally. As criminal networks are borderless and quick to adapt to law enforcement, no nation can fully combat this issue alone.

In order to increase global collaboration, protect cybersecurity, create effective legal processes, and protect those who are victims of online crime, action needs to be taken. However, governments also need to ensure any actions taken to reduce criminality do not infringe on human rights and online privacy.

The delegates have the opportunity to provide realistic solutions to this problem. They can encourage global collaboration and ensure there is a balance between protecting individuals and maintaining their freedoms. The committee can work together with respectful debate to create strategies that combat the causes and effects of the online black market.

This is a global issue; however, there is an opportunity for change. Delegates can work together to create a safer, secure, and responsible digital world.

References

Aqrawi, M., Bazilian, D., & Widdershoven, C. (n.d.). *The World's Most Dangerous Black Markets | YaleGlobal Online*. YaleGlobal Online. Retrieved October 29, 2026, from https://archive-yaleglobal.yale.edu/content/worlds-most-dangerous-black-markets

Besta. (2025, May 30). *Visualizing the World's $12.5 Trillion Underground Economy*. Visualizing the World's $12.5 Trillion Underground Economy. https://besta.com.co/visualizing-the-worlds-12-5-trillion-underground-economy/

ESET Blog. (2025, July 08). *What is the dark web? How it works, and how to access it safely*. ESET. Retrieved October 29, 2026, from https://www.eset.com/blog/en/home-topics/privacy-and-identity-protection/what-is-the-dark-web/

European Union Agency for Criminal Justice Cooperation. (2019, June 01). *Common challenges in combating cybercrime, as identified by Eurojust and Europol*. Common challenges in combating cybercrime, as identified by Eurojust and Europol. https://www.eurojust.europa.eu/publication/common-challenges-combating-cybercrime-identified-eurojust-and-europol?utm_source=

Europol. (2026). *European Cybercrime Centre - EC3*. Europol. https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment?utm_source=

Europol. (2026). *Internet Organised Crime Threat Assessment (IOCTA)*. IOCTA. https://www.europol.europa.eu/crime-areas/online-fraud-schemes/fraud-against-payment-systems

Kosinski, M. (n.d.). *¿What is the dark web?* IBM. Retrieved October 29, 2026, from https://www.ibm.com/mx-es/think/topics/dark-web

Marchini, C. S. (2025, May 27). *The digital drug revolution: How online markets are reshaping global illicit trade*. Global Initiative Against Transnational Organized Crime. Retrieved October 29, 2026, from https://globalinitiative.net/analysis/digital-drug-revolution-online-markets-global-illicit-trade-ocindex/

Sherloc. (n.d.). *Cybercrime trends*. Sherloc. https://sherloc.unodc.org/cld/ar/education/tertiary/cybercrime/module-1/key-issues/cybercrime-trends.html?utm_source=

United Nations Office On Drugs and Crime. (n.d.). *About us*. UNODC. Retrieved October 29, 2026, from https://www.unodc.org/unodc/en/about-unodc/index.html

United Nations Office on Drugs and Crime. (n.d.). *Transnational Organized Crime*. UNODC. Retrieved October 29, 2026, from https://www.unodc.org/unodc/en/organized-crime/toc.html

United Nations Office on Drugs and Crime. (n.d.). *United Nations Convention against Cybercrime*. UNODC. Retrieved October 29, 2026, from https://www.unodc.org/unodc/en/cybercrime/convention/home.html

United Nations Peace and Security. (n.d.). *Basic facts about the global cybercrime treaty*. Basic facts about the global cybercrime treaty. https://www.un.org/en/peaceandsecurity/basic-facts-about-global-cybercrime-treaty?utm_source=

United Nations. (2026). *United Nations Office on Drugs and Crime Liaison Office in Brussels*. United Nations. https://unric.org/en/unbt-agencies/unodc

UNODC.(2026). *About Us. UNODC*. Retrieved November 3, 2026, from https://www.unodc.org/southernafrica/en/sa/about.html