CACI

EVER VIGILANT™

DARKBLUE INTELLIGENCE SUITE

Disrupting Fentanyl and precursor trafficking with dark web intelligence

WHITEPAPER

March 2024

Table of Contents

Executive Summary

The United States is grappling with a critical national safety and security crisis, as the rapid escalation in the proliferation of fentanyl, its analogues, and their precursor chemicals presents an unprecedented challenge. In 2022, the nation experienced a concerning surge in overdose fatalities linked to fentanyl, surpassing 73,000 incidents.

This distressing trajectory not only persisted but also intensified throughout 2023, underscoring an urgent need for comprehensive strategies to address this growing crisis. These strategies must include the ability to identify and target threat actors, illuminate threat networks, facilitate digital underground undercover operations, and enable the identification and development of specific selector leads that result into actionable intelligence in support of the information advantage.

The challenge is exacerbated by the utilization of the dark web ecosphere of influential obfuscation and anonymization technologies through the use of anonymous cyber-domain ungoverned environments, the digital underground, end-to-end encrypted messengers, and social media platforms. Together they create pathways of illicit activities which enable illicit threat actors to transition their operations from open-air markets to these cyber conduits supporting the trade of fentanyl analogs and its precursor chemicals. Using the global reach of the illicit cyber pathways, these substances are frequently transported to Mexico—primarily through the Sinaloa and Cartel Jalisco New Generation (CJNG) cartels—and directly to consumers in the U.S., bypassing traditional surveillance and control mechanisms.

Analytical insights from drug seizure and capture data by the U.S. Drug Enforcement Administration (DEA), the Customs and Border Protection (CBP), the Centers for Disease Control and Prevention (CDC), and the United Nations Office on Drugs and Crime (UNODC) shed light on the dynamics of drug trafficking on a global scale using the dark web. They also highlight the critical necessity of evolving policy measures that effectively counteract the smuggling of these lethal substances.

The situation underscores the urgent need for viable solutions to combat, disrupt, and curb the trafficking of dangerous synthetic opioids like fentanyl. Therefore, response strategies must be adaptable and comprehensive, addressing the physical and digital dimensions of this multifaceted threat.

In the face of the growing opioid crisis, a strategic reshaping of our operational approach is imperative. Key to a robust, effective response are three pivotal strategies, which emphasize the transformative power of technology and the use of dark web intelligence in the global fight against combating the fentanyl epidemic:

1. **Implement Technology**
   Advancing the use of technological capabilities is paramount. The IC OSINT Strategy 2024-2026 [i] underscores the critical role of Open-Source Intelligence (OSINT) in enhancing analytical capabilities. By embracing state-of-the-art technologies, such as artificial intelligence and machine learning, we can significantly improve the ability to analyze vast datasets, detect patterns, and anticipate potential threats. This tech-forward approach is essential for a comprehensive strategy to combat the opioid epidemic effectively.

2. **Leverage Data**
   Utilizing available data intelligently is crucial for crafting targeted, impactful strategies to mitigate the opioid

crisis. Strategic insights, as outlined in the National Intelligence Strategy 2023, [ii] demonstrate how data-driven decision-making can enhance our understanding and response to this complex issue.

3. **Integrate Expertise**
   Collaborative expertise across agencies is essential for a unified, efficient response. Accelerating the fight against the U.S. fentanyl crisis requires breaking down silos and pooling knowledge ensuring a seamless, comprehensive analysis that provides an information advantage against the illicit pathways used by the multifaceted networks driving the opioid epidemic.

Introduction

Fentanyl poses an unprecedented and growing threat to the national security, citizens, and the stability and health of the United States. In 2022, this lethal global threat claimed the lives of over 73,000 individuals[iii] in the U.S. (Figure 1), and the trend persisted and intensified in 2023 (Figure 2). As Department of Homeland Security (DHS) stated in March 2023, the record number of fentanyl overdoses in the U.S. is the "single greatest challenge we face as a country." [iv]

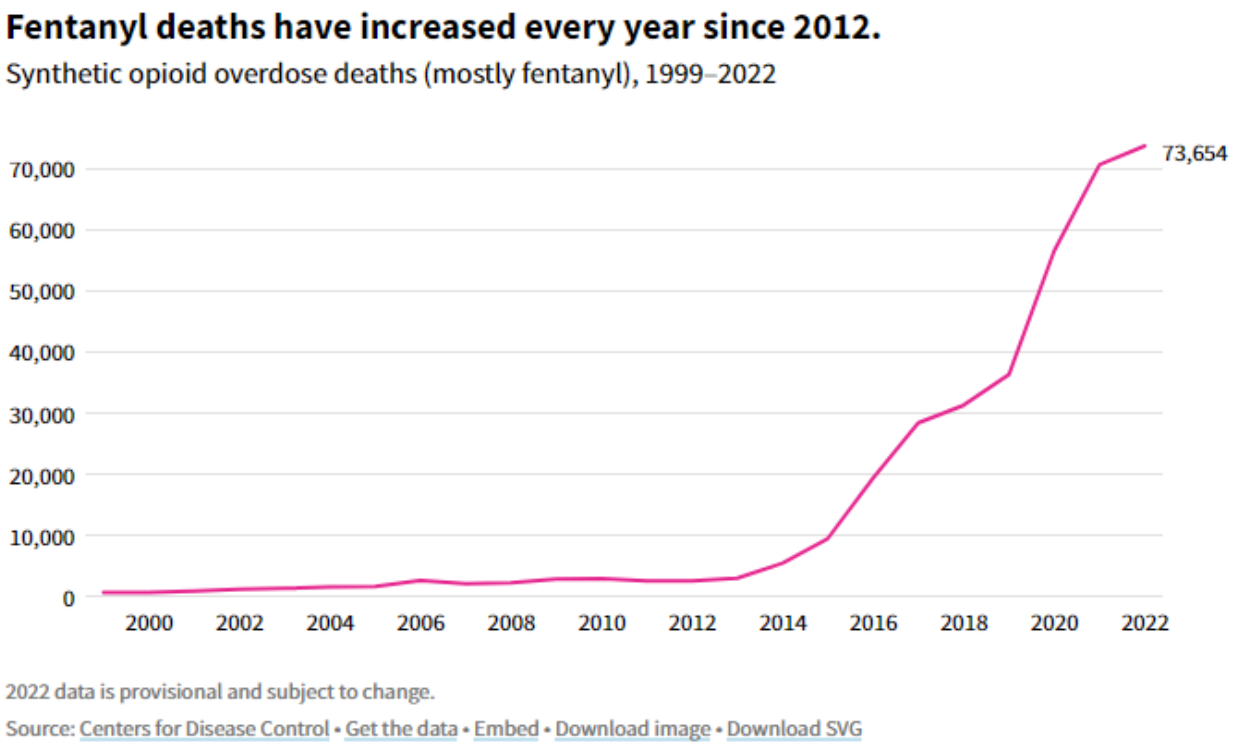


Figure 1: The 2022 Synthetic Opioids death statistics according to the CDC [v]

The CDC employs the 10th Revision of the International Classification of Diseases (ICD-10) to meticulously monitor drug overdose data statistics. This classification system aggregates fentanyl overdoses fatalities alongside those resulting from other synthetic opioids. However, the CDC acknowledges that fentanyl is responsible for the majority of deaths within the synthetic opioid category. It is important to note that drug overdose fatalities often involve multiple substances, hence a single death may be classified under several ICD-10 categories to reflect the involvement of specific drugs in the overdose incident. This nuanced approach ensures a comprehensive understanding of the factors contributing to drug overdose deaths.

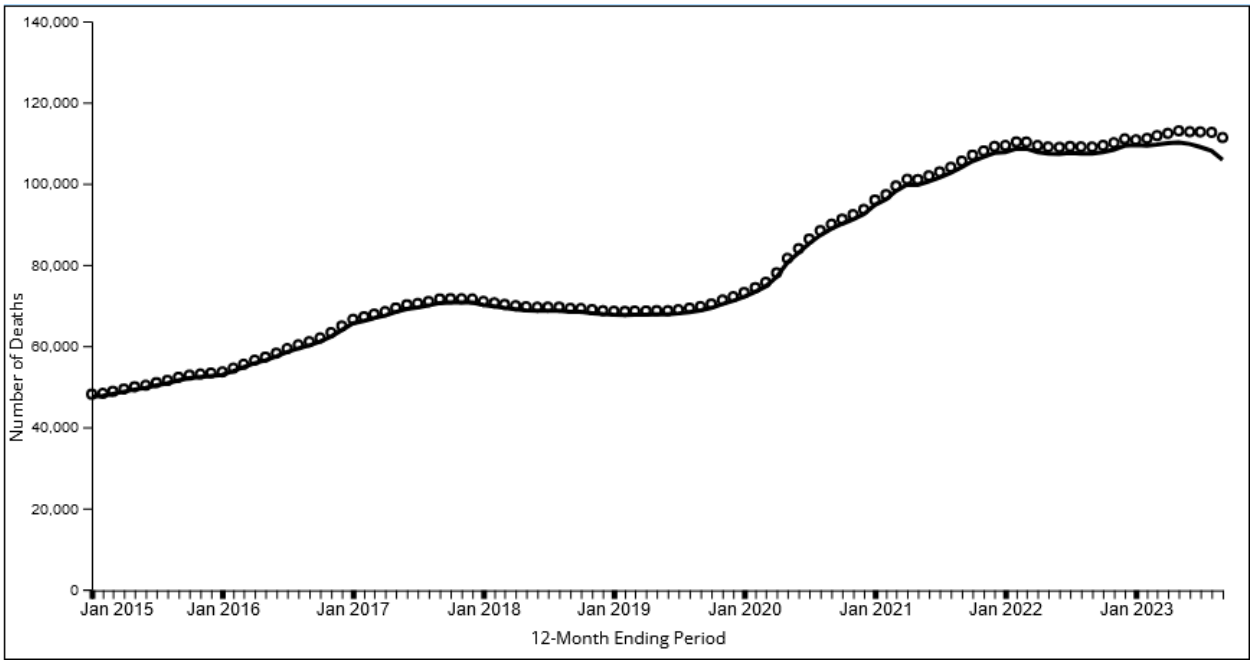


Figure 2: Synthetic Opioids death statistics through January 2023 according to the CDC [vi]

Analytical intelligence also provides valuable insights into drug trafficking dynamics and emphasizes the need for adaptive policy responses to combat drug smuggling, especially potent substances like fentanyl, its analogues, and their precursor chemicals, which are traded openly on the dark web by transnational criminal organizations and threat networks with a global reach.

Such networks implement standard and non-standard logistics supply chains for the movement of synthetic opioids like fentanyl and its precursors directly to those who develop, manufacture, distribute, and consume fentanyl and other synthetic opioids within the United States.

The complexity of this threat – which the Department of Homeland Security (DHS) considers a "red-alert moment," [vii] is further compounded by an uncooperative Chinese government, the international trafficking of fentanyl and fentanyl precursors to Mexico by the Sinaloa and Cartel Jalisco New Generation (CJNG) cartels, and the illicit digital-domain trade networks on the dark web that enable vendors to market fentanyl analogues and its precursor chemicals under the auspice and obfuscation and relative anonymity encrypted networks provide.

Exploiting dark web intelligence to target these threat actors and illuminate their networks, facilitate operations in the digital underground, and develop actionable intelligence requires several technical, analytical, and operational approach methods to gain an information advantage.

Case Studies and Data Analysis

CACI research on deep and dark web fentanyl and other synthetic opioid trafficking has revealed key identifiers like exposed credentials, email addresses, cryptocurrency addresses, shipment tracking numbers, and Google Analytics IDs. These exploitable opportunities enable law enforcement to link online dark web vendors to their real-world identities and activities using a pathway defeat approach.

There are three pathways for selling substances on digital ungoverned environments:

1. **Forums:** Individual threat actors selling on darknet sites operated by an individual or a group of individuals.
2. **Marketplaces:** Online marketplaces that act as a medium for connecting buyers and sellers.
3. **Direct-to-Consumer:** Individual sellers under the guise of anonymity connect and sell direct-to-consumer using the darknets to facilitate secure transactions.

By analyzing these identified nodes and leveraging interagency and commercial partners, U.S. law enforcement and international partners can deanonymize these targets, understand the threat networks, track geolocations, and connect cargo shipping histories, thereby facilitating operations to dismantle these illicit networks. The ability to intercept and disrupt the flow of fentanyl and its precursor chemicals will deny Mexican transnational criminal organizations the ability to control the trade. This action will also jeopardize their capabilities to communicate with established trafficking networks through criminal groups and gangs, both on and off U.S. territories.

These methods, which are highlighted in the following case studies, are repeatable and effective in targeting and deanonymizing these threat actors, and crucial for monitoring markets, forums, and known threat actors using new and established transportation trends, movement, and distribution networks.

CASE STUDY 1: CHINESE CHEMICAL COMPANY

On 31 July 2023, CACI analysts identified Chinese Chemical Company (1)—a research chemical company based in Hubei Province[viii], China—as one of the largest suppliers of fentanyl precursors on the preeminent dark web chemical forum and marketplace Breaking Bad. Chemicals available include numerous variations of 4-piperidone and other fentanyl precursors identified in recent actions by the DOJ and the Department of the Treasury (TREAS). [ix]

Figure 3: Shipment tracking numbers for successful deliveries by Canada Post

Comprehensive analysis and defined research workflows enabled CACI analysts to identify numerous selectors associated with the company, including Chinese mobile phone numbers, social media IDs, instant messaging handles, and two public websites. In addition to these selectors, shipment tracking IDs were also identified. These tracking IDs create traceable paths back to the individuals involved in shipping and purchasing, providing an opportunity to disrupt the supply chain.

CASE STUDY 2: DARK WEB VENDOR

With a deep understanding of how dark web vendors source and traffic synthetic opioids in ungoverned digital spaces, CACI analysts identified a Dark Web Vendor as a U.S.-based drug trafficker selling Mexican cartel-supplied pills and heroin laced with fentanyl on several darknet markets.

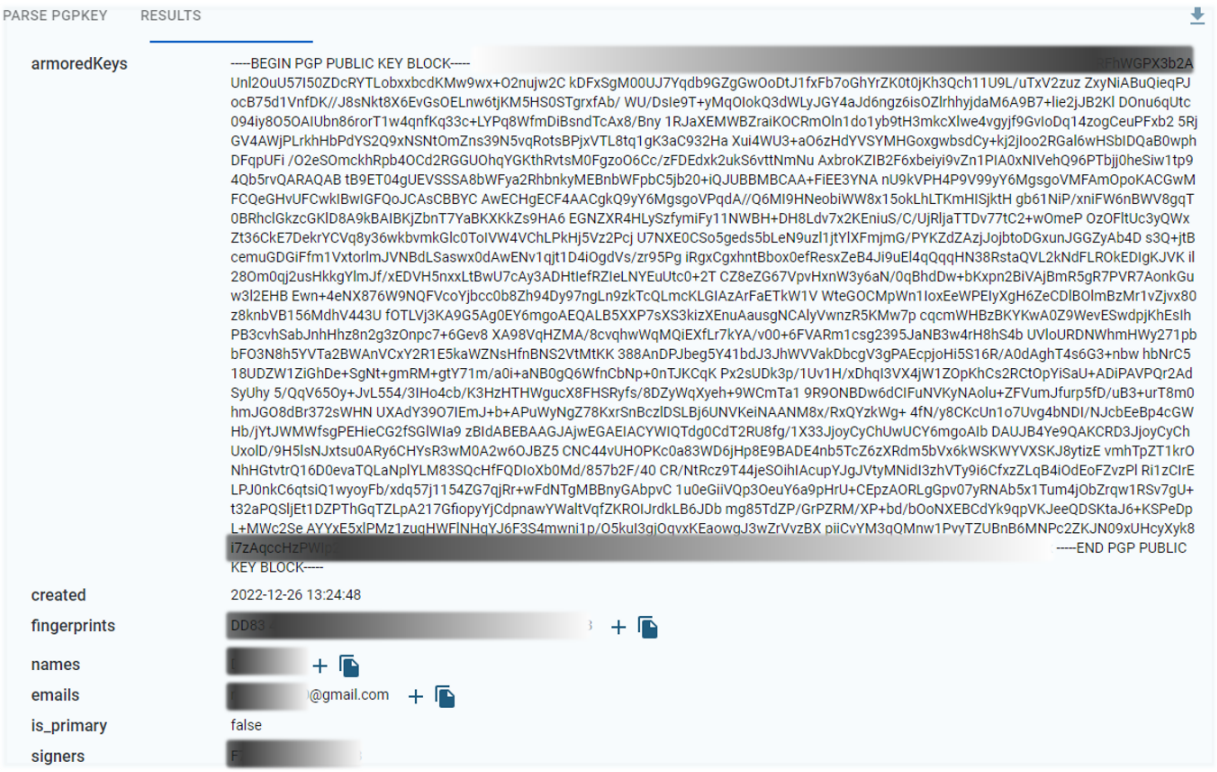


Figure 4: Parsed PGP key identifying a Gmail address belong to the vendor

Leveraging DarkBlue data, CACI analysts uncovered a PGP key, Gmail addresses, U.S. mobile phone numbers, and a Snapchat account connected to the threat actor. Subsequent research in the live environment using DarkPursuit linked these selectors to a probable real-world identity and presented law enforcement with the opportunity to dismantle an illegal network and curtail the sale of dangerous synthetic opioids that pose a grave threat to public health and safety.

CASE STUDY 3: PILL PRESS SUPPLIER

A great first step in attacking the fentanyl crisis is a systematic analysis of all aspects of the problem set by analyzing, illustrating, and illuminating the entire synthetic opioid value chain. In March 2023, CACI published a comprehensive report identifying a Chinese company selling illicit drugs, precursor chemicals, and pill press machines on the open and dark web. Pill press machines play a pivotal role in the global fentanyl supply chain, from production in Mexico to smuggling and distribution in the United States. Removing these machines from the supply chain would disrupt illicit manufacturers' ability to easily and rapidly produce large quantities of fake prescription pills.

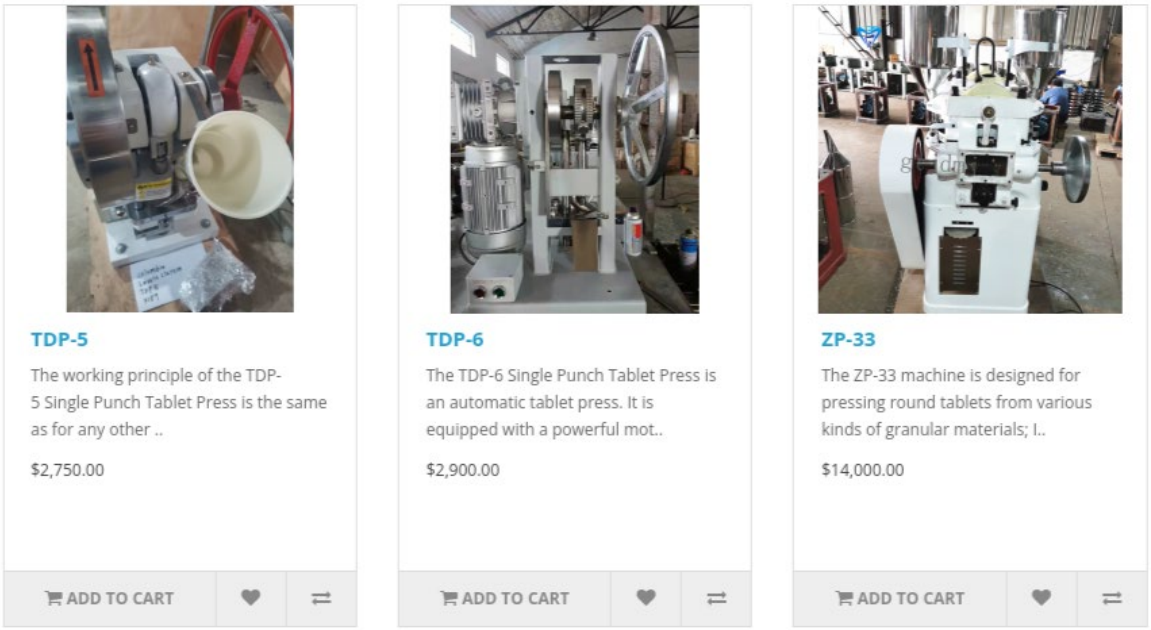


Figure 5: Pill presses offered for sale on the dark web site by the manufacturer

By employing the DarkBlue Intelligence Suite, CACI analysts quickly and safely identified exposed credentials for an encrypted email address and the Google Analytics tracking IDs on their Tor site. These IDs could potentially provide law enforcement with opportunities to link the market to its creators and their identities outside of the dark web and remove a crucial aspect of the synthetic opioid value chain.

CASE STUDY 4: CHINESE CHEMICAL SUPPLIER 2

Chinese Chemical Supplier 2 is a research chemical company headquartered in the Kowloon area of Hong Kong with a strategic geographical sales approach targeting Mexican and Dutch clients. Identified by CACI analysts in late July 2023, the company operates several public websites and maintains a presence on dark web forum and marketplace Breaking Bad. Precursor chemicals offered for sale include 1-N-Boc-4-phenylaminopiperidine (CAS: 125541-22-2) [x] and 1-Boc-4-piperidone (CAS: 79099-07-3), which were highlighted in recent actions by the U.S. DOJ and TREAS targeting Chinese suppliers of fentanyl precursors. [xi]

Figure 6: Fentanyl precursor advertised on supplier's Spanish-language dark web site

A targeted scrape of one of the company's open web sites identifies an exposed Google Analytics ID. This selector may assist in identifying site owners, establishing connections to illegal sales of fentanyl precursors, and illuminating behaviors tracked by Google Analytics to gather evidence supporting the company's illegal activities. Additionally, collaboration with Google services enables access to further details associated with the Analytics ID, such as IP addresses or user behavior, supporting efforts to track and potentially shut down the company under applicable laws and jurisdictional regulations.

CASE STUDY 5: CHINESE CHEMICAL SUPPLIER 3

In early September 2023, CACI analysts identified Chinese Chemical Supplier 3 as a primary supplier of fentanyl precursors and other synthetic opioids to U.S. and international clients on the open and dark web marketplace and forum Breaking Bad. The company—which is based in Anhui Province, China—includes 1-Boc-4-piperidone (CAS: 79099-07-3) for $200 USD per kilogram in its product listings.

Figure 7: Various precursor chemicals advertised on supplier's company website

Additionally, they guarantee "100% secure delivery, no customs issues" to the United States, Mexico, Canada, and other countries. Using DarkBlue and DarkPursuit, CACI identified several Chinese mobile phone numbers and a Gmail address within the company's advertisements. As law enforcement agencies implement measures to curb traditional drug trafficking routes, drug suppliers are increasingly turning to the dark web and encrypted communication platforms to evade detection. These selectors present ample opportunity to illuminate the synthetic opioid value chain via signals intelligence, data exploitation, and analytical discovery.

CASE STUDY 6: CHINESE CHEMICAL SUPPLIER 4

Chinese Chemical Supplier 4 is a research chemical company based in Hubei Province, China that operates on the open and dark web. Offering fentanyl precursors, Xylazine, and other dangerous substances, the company claims to have warehouses in the United States, Mexico, Canada, Russia, Germany, and Australia for local distribution. Products available include at least six variations of 4-piperidone, a major precursor for fentanyl. A review of the company's sales representatives identified an individual with a prior affiliation with Hubei Amarvel Biotech Co. Ltd. (AmarvelBio), a company that was recently indicted by the DOJ for supplying fentanyl precursors to Mexican cartels.

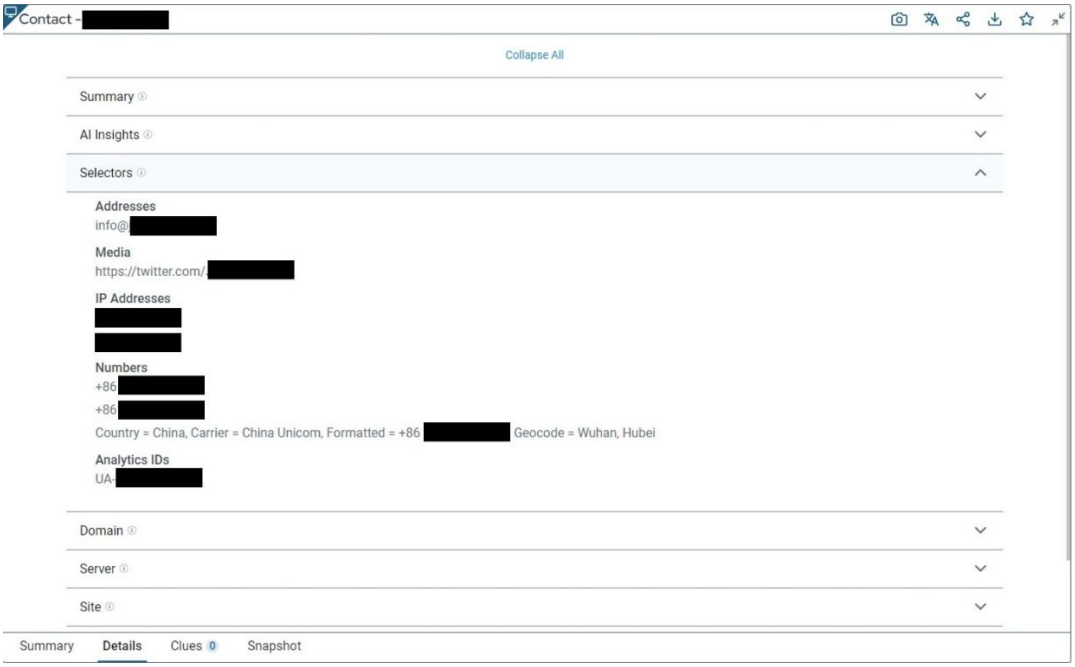


Figure 8: Selectors for supplier revealed after targeted scrape of company's website

CACI analysts conducted targeted scrapes of the company's public websites and profiles on Breaking Bad using DarkPursuit Capture, revealing numerous selectors of interest. These include open web sites, a Google Analytics ID, mobile phone numbers, email addresses, and instant messaging IDs. Law enforcement can leverage these opportunities to enhance their understanding of this threat network, trace geolocations, and effectively target its distribution network.

The Challenge

Synthetic opioids such as fentanyl and its analogs are primarily manufactured in nations with expansive pharmaceutical and chemical sectors with lenient regulatory oversight. The high profitability of fentanyl compared to other drugs, coupled with the growing demand of easy-to-access digital domain illicit markets, motivates producers to continue manufacturing the synthetic opioid and its analogs despite legal risks. The regulatory landscape in some Asian countries may also contribute to the challenge of controlling fentanyl production. Weak regulations, corruption, and inadequate enforcement mechanisms create loopholes that illicit producers exploit to operate clandestine laboratories.

Despite the restrictions against the export of fentanyl and other synthetic drugs placed by China in May of 2019, [xii] CACI analysts have identified Chinese vendors who have tapped into online networks to market fentanyl analogs and precursor chemicals and ship them directly to customers in the U.S., Mexico, U.K., and Europe as well as to Mexican cartels. [xiii] Obscured by a vast network of legitimate chemical and pharmaceutical companies producing a wide array of compounds and substances, Chinese manufacturers exploit international trade routes and the anonymity of the internet—particularly the deep and dark web—to market and distribute precursor chemicals to various regions worldwide, facilitating the production of synthetic opioids far beyond China's borders.

India has also emerged as a noteworthy participant in fentanyl production due to its robust pharmaceutical industry and proficiency in chemical synthesis. The nation's pharmaceutical infrastructure, combined with the availability of precursor chemicals from China, has significantly contributed to the production of fentanyl and its analogs. Following the crackdown on fentanyl precursors 4-anilino-N-phenethyl-4-piperidine (ANPP) and N-phenethyl-4-piperidone (NPP) by the Chinese government in 2018, the DEA noted a shift in production of fentanyl from China to India. [xiv] While India has since scheduled these precursors, the vast pharmaceutical infrastructure allows covert laboratories to continue manufacturing synthetic opioids and supplying them to cartels in Mexico and directly to customers in the United States.

The U.S. Government's capability to leverage critical yet expansive and frequently siloed data on this threat is constrained by limited analytical resources. The design of the U.S. intelligence community initiatives frequently underdelivers in effectively supporting law enforcement objectives due to the sheer scale of the data on-hand. Challenges include compartmentalized and poorly coordinated intelligence efforts that hinder lawful identification and targeting of the extensive and malign networks supporting this menacing threat. The U.S. law enforcement agencies (LEAs) community confronts these obstacles as the scale and severity of the fentanyl crisis pose increasing challenges to a broader segment of the U.S. Government and its national interests.

LAW ENFORCEMENT ACTIONS AND RESPONSE

The synthetic opioid crisis has exacerbated the already-critical drug epidemic in the United States, marking a significant escalation in the nation's long-standing battle against the proliferation of synthetic opioids. This phenomenon has precipitated the deadliest drug crisis in American history, compelling the DEA, the Federal Bureau of Investigation (FBI), Department of Homeland Security including Homeland Security Investigations (HSI), Customs and Border Patrol (CBP), Department of Justice (DOJ), and other U.S. LEAs to intensify their efforts in combating opioid-related criminal activities. In response to this alarming situation, U.S. LEAs have augmented their arsenal with innovative resources, taking note of the opportunities that dark web intelligence offers law enforcement and the greater intelligence community.

The dark web has impacted the illicit goods and services supply chain, and the constantly evolving nature of cybercrime challenges traditional law enforcement methods. The dark web's influence on the drug trade of fentanyl and other synthetic opioids through the sale and distribution of pre-cursor chemicals, is significant due to several factors:

1. It offers a cost-effective, global platform for promoting products, including new drugs and consumption methods.
2. Advanced information and communication technologies facilitate anonymous operations and secure communications, playing a crucial role in covert drug marketplaces.
3. The dynamic online environment continuously spawns novel methods for drug distribution, outpacing law enforcement efforts.

These factors have shaped the dark web: a formative, virtual, ungoverned digital markets ecosystem that commonly serves as an anonymous, global black market for illicit goods and services where drugs, weapons, and fraud are commonplace. Within this domain, technological innovation is seamless. Threat actors can provide an obfuscated, secure shopping experience for illegal goods and services. Ultimately, its marketplaces have become a place to test demand for new products and untested, unregulated substances not seen in open-air markets.

The U.S. Government and the international law enforcement community focus on the dark web to combat the trade of fentanyl and synthetic opioid substances and pre-cursor chemicals for several reasons:

- **Anonymity of the dark web:** The dark web is known for its high degree of anonymity, making it a preferred platform for illegal activities, including the trade of synthetic opioids like fentanyl. Targeting this space, law enforcement should seek to penetrate key zones where these activities thrive.

- **Prevalence of Opioid Trafficking Online:** With the rise of the opioid crisis, a significant portion of trafficking has moved online, particularly to the dark web. This shift necessitates a corresponding pivot in law enforcement strategies that effectively tackle the issue.

- **Network Infiltration and Intelligence Gathering:** Cyber reconnaissance and intelligence gathering operations indicate law enforcement efforts to infiltrate these networks, suggesting a proactive approach to intelligence gathering, which is crucial for understanding and dismantling the operational mechanisms of the illegal opioid trade.

- **Dismantling Online Marketplaces:** The dark web hosts numerous marketplaces that facilitate the sale of illegal drugs like fentanyl. By focusing on these online spaces, U.S. LEAs aim to disrupt the supply chain of opioids, impacting the overall availability and distribution of these substances.

- **Specialized Focus on Online Trafficking:** The significant increase in resources dedicated to U.S. LEAs—including more special agents, intelligence analysts, and professional staff—indicates a focus on online opioid trafficking. This specialization is essential due to the unique challenges posed by cyber environments and the digital criminal underground.

With these conditions in mind, the DOJ and other federal agencies built, shaped, and established the Joint Criminal

Opioid Darknet Enforcement (JCODE) team to intercept, disrupt, and neutralize fentanyl trade on the dark web. JCODE serves as a specialized unit that employs cutting-edge technological resources and collaborative methodologies, harnessing and implementing dark web intelligence to effectively dismantle and neutralize the rapidly expanding darknet marketplaces for illegal opioids. This focused approach positions the DOJ and U.S. LEAs at the forefront of the national effort to combat the opioid epidemic, targeting a critical and evolving battleground in this public health crisis by taking advantage of the dark web intelligence opportunities.

HIGHLIGHTS OF JCODE SUCCESSES

Since its inception in 2017, JCODE has been led by the FBI, the primary agency within the initiative under the DOJ. They have had significant success operating on the dark web. These operations have consistently brought results and illuminated key issues in combating the fentanyl crisis. The success of the JCODE team can be highlighted in several key areas:

1. **Enhanced collaboration:** JCODE has successfully cultivated collaboration with various U.S. LEAs, adopting an interagency approach that involves federal, state, and local entities. This strategy has led to more effective measures in tackling opioid trafficking, particularly those related to the dark web.

2. **Increased arrests and prosecutions:** Since its inception, JCODE has been instrumental in increasing the number of arrests and prosecutions of individuals involved in illegal opioid sales on the dark web, including both small-scale and large-scale dealers.

3. **Disruption of darknet operations:** JCODE operations have resulted in the disruption of numerous darknet marketplaces. These disruptions hinder the ability of drug traffickers to use these platforms for selling opioids and other illegal substances.

4. **Public awareness and outreach:** Apart from enforcement actions, JCODE has played a role in raising public awareness about the dangers of opioid abuse and the role of the darknet in fueling the opioid crisis. Their efforts have extended to educational campaigns targeting potential users and communities.

5. **Technical expertise and innovation:** Their technical expertise in navigating and investigating the dark web has led to the creation and application of innovative techniques for tracking and apprehending individuals engaged in these clandestine operations.

6. **International Cooperation:** JCODE collaborates with international LEAs for international operations, a vital component given the borderless nature of the internet and darknet operations.

7. **Significant Seizures:** The team has been responsible for significant seizures of illegal opioids, which not only disrupt the supply chain but also prevent these drugs from reaching the streets and potentially causing overdoses.

The success of JCODE is rooted in its approach to addressing the darknet-facilitated opioid crisis, which includes a broad dark web intelligence adoption approach; the use of specialized tools for safe, secure access to the live operating environment; and the development of specialized technical expertise using on-demand collection methods that capture the illicit activities taking place on the dark web and their pivot points into the physical world open air markets.

The following sections highlight several successful JCODE missions.

Operation SpecTor (May 2023)
Operation SpecTor was conducted by law enforcement in the U.S., U.K., Brazil, and Europe to target Monopoly Market, a major darknet drugs marketplace. [xv] International police arrested 288 suspects and recovered more than 50 million euros in cash and virtual currency.

Figure 9: A map of the operations against drug traffickers operating on the darknet [xvi]

Operation DarkMarket (January 2021)
DarkMarket, previously the world's largest illegal marketplace on the dark web, [xvii] was taken offline in an international operation involving Germany, Australia, Denmark, Moldova, Ukraine, the U.K. (the National Crime Agency), and the U.S. (DEA, FBI, and Internal Revenue Service).

The European Union Agency for Law Enforcement Cooperation (Europol) and the European Cybercrime Centre (EC3) supported the takedown with specialist operational analysis and coordinated the cross-border collaborative effort of the countries involved. [xviii]

Figure 10: The homepage of DarkMarket after it was taken offline [xix]

Operation DisrupTOR (September 2020)
The JCODE team—along with Europol—conducted Operation DisrupTor, a coordinated international effort to disrupt opioid trafficking on the dark web.

The mission was operated by the U.S. and Europe and demonstrates their continued partnership against the illegal sale of drugs and other illicit goods and services.

Figure 11: Statistics from Operation DisrupTor [xx]

Operation SaboTor (March 2019)
The JCODE team released the results of Operation SaboTor, a coordinated international effort targeting drug trafficking organizations operating on the dark web. [xxi] The U.S. and international LEAs made more than 61 arrests and shut down 50 darknet accounts.

Law enforcement executed 65 search warrants, seizing 299.5 kilograms of drugs, 51 firearms, and approximately $6 million USD ($4.5 million in cryptocurrency, $2.48 million USD, and $40,000 in gold).

Figure 12: An image of the perception versus reality of buying on the dark web [xxii]

Operation Disarray (April 2018)

Operation Disarray was a first-of-its-kind operation by the DOJ and JCODE that aimed to underscore the risks for buyers and sellers on the dark web. This operation involved a coordinated effort by hundreds of FBI agents and federal partners, including the DEA, CBP, Internal Revenue Service (IRS), DHS, and U.S. Postal Inspection Service. The operation executed searches, arrests, and conducted "knock and talks" with over 160 individuals identified [xxiii] as having purchased or sold drugs via these marketplaces. [xxiv] The investigation yielded leads that pointed to 19 overdose fatalities among the persons of interest.

Figure 13: Screenshot of the PR promotion for Operation Disarray on the dark web

The Global Dark Web Problem

The shipment of fentanyl and its precursors from China and India to Mexico and the United States involves a variety of methods and routes facilitated by the global interconnectedness of trade, ungoverned digital spaces, and the sophisticated tactics employed by the traffickers. The process involves a complex network of transportation, concealment, corruption, and distribution orchestrated by the suppliers to ensure the flow of illicit drugs across international borders and through many continents making this a global problem.

Furthermore, the U.S. federal law enforcement response faces daunting challenges due to the complexity of combating fentanyl distribution. While the U.S. Government and the international community have achieved notable success in disrupting and neutralizing fentanyl pathways, effectively utilizing valuable dark web data remains a significant challenge. The vast amount of data generated as a result of these efforts often remains segregated, hindered by the limited analytical resources available within the U.S. Government. The growing scale and intensity of the fentanyl threat increasingly challenge large parts of U.S. LEAs and tests the capacities of an expanding segment of the U.S. Government. These persistent challenges are attributable to these key factors:

- **Complexity of the dark web:** The dark web, where much of the illegal fentanyl trade occurs, is complex and constantly evolving as the technologies and methods used by traffickers often change.
- **Anonymity and Encryption:** The use of sophisticated encryption and anonymity tools by sellers and buyers on the dark web makes it difficult to trace and apprehend individuals involved in the fentanyl trade.
- **Global Nature of the Problem:** Fentanyl trafficking often involves international networks, requiring coordination across multiple jurisdictions and legal systems, which can be complicated and time-consuming.
- **Resource Intensive:** Effective dark web investigations require significant resources—including specialized training, technology, and personnel—which may not be available for some law enforcement agencies.
- **Rapidly Shifting Marketplaces:** Darknet marketplaces can shut down and re-emerge under new names on different servers, creating challenges in monitoring and controlling these platforms.
- **Legal and Ethical Considerations:** Operations on the dark web raise questions about privacy and surveillance and require balancing effective enforcement with respect for civil liberties and the limits of law enforcement.
- **Post-Seizure Implications:** Successful operations that shut down marketplaces or catch dealers sometimes only temporarily impact the overall availability of fentanyl as new players quickly fill the void.

These challenges are confounded by the following problems.

1. Synthetic opioids moved manufacturing from the field to the lab

The evolution of illegal drug manufacturing from open-field cultivation to clandestine laboratory operations presents a significant challenge for law enforcement and drug policymakers. In the past, the production of drugs like cocaine and heroin typically involved large-scale agricultural undertakings in remote areas, which—despite their hidden

nature—could still be detected through aerial surveillance or on-the-ground intelligence. However, the shift towards synthetic drugs like methamphetamine and fentanyl has transformed drug manufacturing into a more concealable and mobile activity. Modern laboratories—often set up in urban settings, private residences, or mobile units—are smaller and harder to detect. This transition not only complicates detection efforts but also poses new dangers due to the highly toxic and volatile nature of chemicals used in synthetic drug production. As a result, LEAs must adapt by requiring more sophisticated surveillance techniques, specialized training in chemical identification, and enacting a greater emphasis on intelligence-led policing.

2. Synthetics are easy to make, potent, and profitable

The production of synthetic opioids like fentanyl involves readily substitutable chemicals and evading export-import controls. These opioids are significantly more potent than heroin, enabling traffickers to minimize volume while maximizing profits. Annually, only three to five metric tons of fentanyl are required to meet the U.S. demand for illegal opioids, much less than the consumed quantities of heroin and cocaine. [xxv] [xxvi]

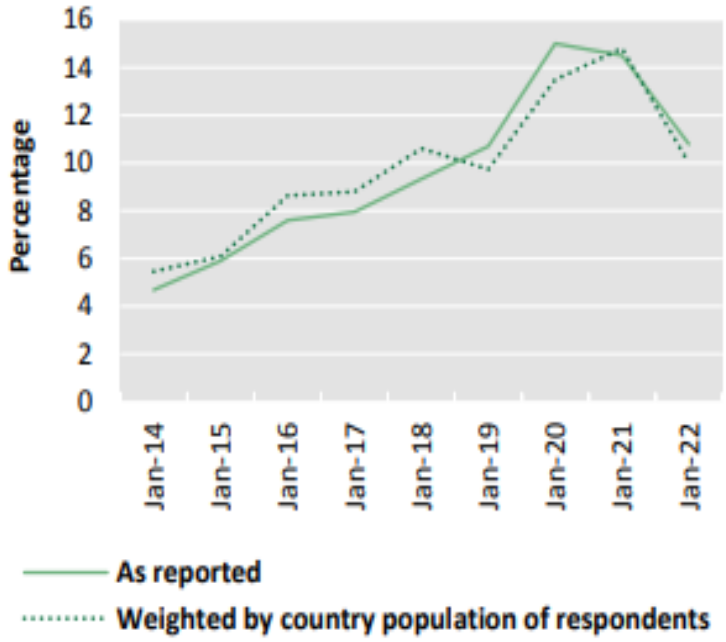
Sources: Kilmer, B. and Reuter, P., 2009. DOPED. *Foreign Policy*, (175), p.34.; and Reuter, P., Pardo, B. and Taylor, J., 2021, "Imagining a fentanyl future: Some consequences of synthetic opioids replacing heroin", *International Journal of Drug Policy*, *94*, p.103086.

Figure 14: Comparison of the labor supply depiction of natural and synthetic drugs [xxvii] [xxviii]

3. Demand continues to drive the supply of synthetic opioids

The demand for synthetic opioids is shaping their supply, with traffickers adapting to consumer preferences. Synthetic opioids, now available in pill form, exploit the familiarity and reduced stigma associated with pill consumption. A major concern is the unsought presence of fentanyl in heroin or counterfeit tablets, mimicking

brands like OxyContin and Xanax, leading to increased overdoses. Effective demand-reduction strategies focusing on opioid misuse and prescription pill abuse is essential to decrease demand and save lives.



Source: UNODC calculations based on Global Drug Survey 2022 data (and previous years): detailed findings on drug cryptomarkets.

Figure 15: UNODC 2022 Survey [xxix]

4. Encrypted platforms and social media make it difficult to disrupt suppliers [xxx]

Global logistics—including postal, courier, and cargo systems—facilitate the movement of precursors and drugs. Smuggling across the U.S.-Mexico border remains the main route for illegal fentanyl, with an increased use of the U.S. mail system for domestic distribution. Compact shipments of pills and new chemicals often evade detection. Law enforcement must depend on costly advanced technologies or conventional methods based on observations and intuition.

The use of social media, encrypted platforms, and established logistics networks complicates the disruption of synthetic opioid distribution. Vendors connect with buyers, such as Mexican cartels, on online platforms and then communicate via encrypted systems inaccessible to law enforcement.

5. Distinguishing between legitimate and illicit uses of precursor chemicals **is difficult**

The DEA manages the use of precursor chemicals under the Controlled Substances Act (CSAA). The DEA may

prosecute violators of this law at both the domestic and international levels. Under the SCA, anyone who orders, handles, stores, and distributes controlled substances must be registered with the DEA to perform these functions. Those entities must maintain accurate inventories, records, and security of the controlled substances. Trustworthy pharmaceutical and chemical suppliers import these precursors for valid medical purposes, such as pain management and anesthesia. However, entities engaged in the illegal manufacture of fentanyl can exploit these same chemicals.

Distinguishing between legitimate and illicit uses of precursor chemicals essential for fentanyl production poses a significant challenge. Identifying the companies using these substances legally requires meticulous scrutiny and oversight, such as verifying the credibility and record of suppliers, monitoring supply chains, and ensuring strict adherence to regulatory standards. The complexity lies in effectively regulating and overseeing the flow of these precursor chemicals without impeding their legitimate medical use, necessitating a nuanced and informed approach from regulatory bodies and law enforcement agencies.

6. Geopolitics stand in the way of actionable solutions to disrupt supply chains

The intricate web of serious geopolitical issues significantly hampers efforts to disrupt the supply of illegal drugs, presenting a complex challenge for international law enforcement and policymaking bodies. The production and trafficking of illicit substances are often deeply entwined with the political and economic fabric of certain regions, where drug revenues can become a critical part of local economies or even fund armed conflicts and insurgent groups.

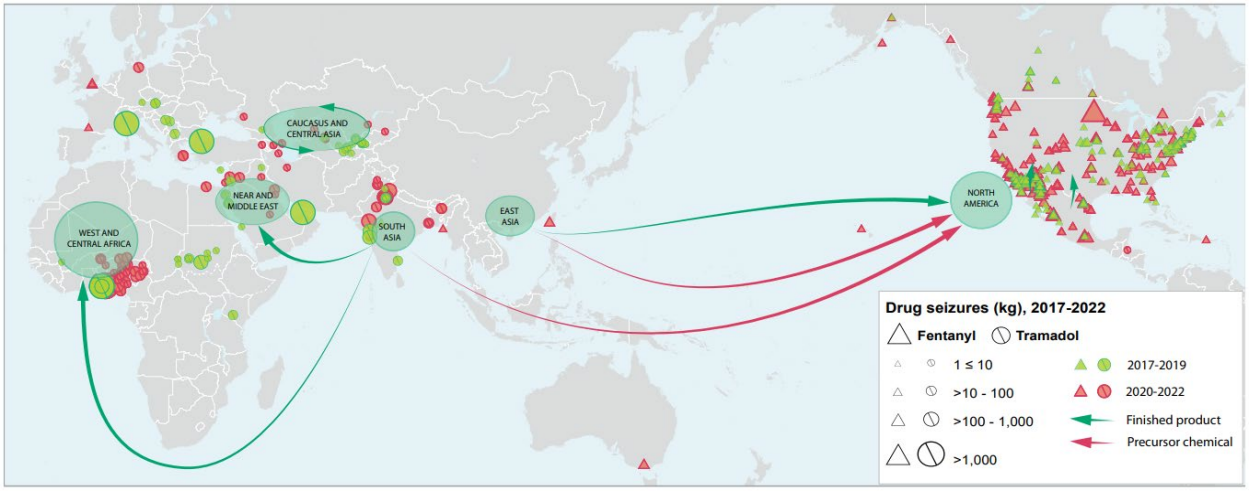


Figure 16: A map of global drug seizures from 2017 to 2022 [xxxi]

Actions to disrupt these supply chains can have far-reaching political implications, affecting diplomatic relations and regional stability. In some cases, the involvement or complicity of corrupt officials and institutions further complicates matters, undermining anti-drug efforts and leading to a delicate balance between enforcing drug laws and maintaining geopolitical stability.

Moreover, international cooperation—which is crucial in combating drug trafficking—can be hindered by differing national policies, legal frameworks, and priorities, making coordinated and effective global responses to drug supply a difficult endeavor. These geopolitical intricacies require a nuanced approach, blending law enforcement action with diplomatic engagement and socio-economic development strategies to address the root causes of drug production and trafficking.

The U.S. Government must seek to analyze emergent trends in drug markets and related behaviors through a systematic and standardized approach. The use of novel, high-frequency, and real-time systems to enhance market surveillance must be considered and implemented.

Solutions

The U.S. Government requires[xxxii] a comprehensive approach[xxxiii] to address the synthetic opioids epidemic and the larger issue of Mexican cartels profiting from their creation and distribution. A comprehensive and innovative approach is essential to address the multifaceted challenges posed by the illegal supply of synthetic opioids. Central to this strategy is the direct involvement of federal agencies in enhancing the understanding of the dynamics within these illicit drug trade and distribution networks and markets.

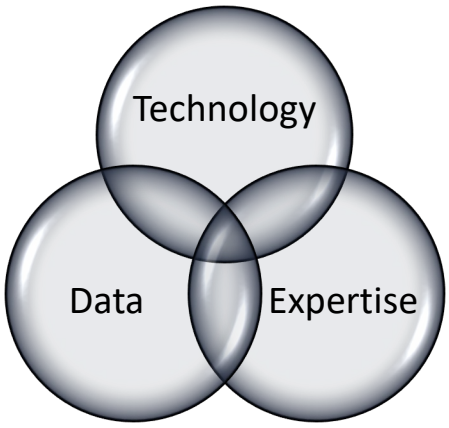


Figure 17: A diagram of a three-step approach to identify illicit goods and services online

The solution requires the ongoing and persistent employment of strategic methods that include law enforcement actions, public health strategies, and international cooperation paired with technology, the collection of relevant data and access to such data on demand. These activities combined with the exploitation of expertise will build and shape the operationalization, tactics and techniques required to combat the effects of the problem at scale.

The limited analytical resources of the U.S. Government hinder its capacity to effectively utilize the vast and frequently disparate data available for exploitation. The nation's intelligence community efforts are often sub-optimally designed to support law enforcement outcomes. Our nation faces challenges such as siloed and least optimally integrated intelligence activities, hindering the lawful identification and targeting of the vast and malicious network-of-networks that undergird this growing and intensifying threat.

These challenges direct federal efforts to improve the understanding of the illegal supply chains of synthetic opioids as pathway defeat mediums. Pathway defeat solutions have proven in the past two decades to be the optimal method for effectively contesting threats that are:

1. Highly networked in nature
2. Dependent on complex combinations of both lawful and illicit supply and resource chains

3. Designed to “hide and operate within” complex combinations of cultural, political, societal, financial, and criminal activities.

The methodological pathway defeat solution is a factor-based systematic analysis of all aspects of the problem at-scale. This would involve identifying, analyzing, illustrating, and illuminating the entire synthetic opioid trade value chain.

The implementation of a pathway defeat approach allows enablers to identify strategic choke points, develop interagency and cross-border international measures to affect those strategic choke points, and position the U.S. to respond and mitigate identified vulnerabilities and contributing factors which effect the synthetic opioid epidemic at-large. This approach aligns with best industry practices and is usable and replicable using the technology, data, and expertise approach to dark web intelligence.

Figure 18: A diagram of a three-step approach to identify illicit goods and services online

This methodology requires not only a focus on the physical trafficking of drugs but also a keen eye on the digital landscape where these transactions increasingly occur. To achieve success in combating the synthetic opioid crisis, the ongoing use, refinement, and operationalization of dark web intelligence across the United States law enforcement and intelligence community landscape is critical.

DARK WEB INTELLIGENCE IN DISRUPTING THE SYNTHETIC OPIOID TRADE

Dark web intelligence involves gathering, analyzing, and utilizing information from the dark web to track, monitor, and report on various activities, particularly within the security, law enforcement, and cybersecurity domains. The dark web is a part of the internet accessible only using special software such as Tor, I2P, Zeronet, and Hyphanet (previously known as Freenet), which helps users and website operators remain anonymous or untraceable. Its anonymity makes it a hub for various illegal activities, such as drug trafficking, weapons sales, cybercrime, and illicit threats and financing.

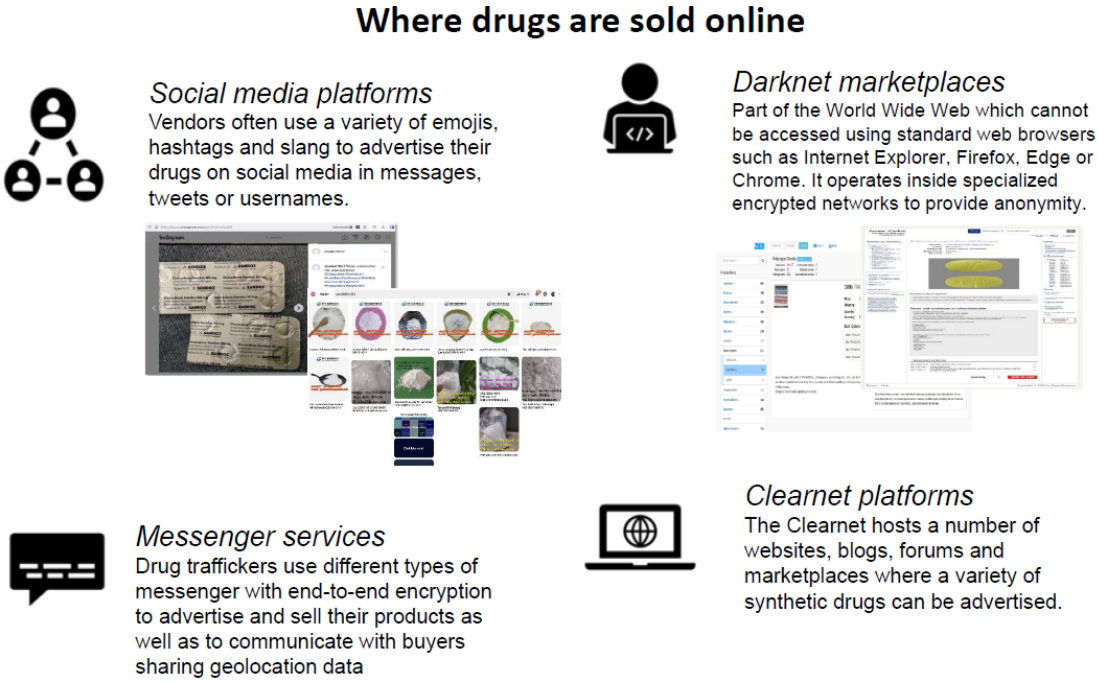


Figure 19 1: Popular selling methods of illicit goods and services online [xxxiv]

A strategic and methodical approach using dark web intelligence is required to combat illicit fentanyl and its precursor chemicals. This approach must leverage the expertise of experts, technology, processes, and data. Additionally, it must support tracing, tracking, and locating illicit distribution networks to highlight supply vectors and illicit pathways that enable the distribution of precursor chemicals used to develop synthetic opioids.

EXPLOITATION OF DARK WEB INTELLIGENCE

The creation and application of specialized ungoverned and unregulated cyber domain monitoring tools are crucial. These tools must scrutinize dark web marketplaces, encrypted messengers, social media platforms, and the anonymous realms of the dark web, which have evolved into hotbeds for the trade in precursor chemicals and synthetic opioids.

LEAs can effectively track and flag suspicious online activities by partnering with technology companies and utilizing advanced software with artificial intelligence (AI) and machine learning (ML) capabilities. This digital vigilance is complemented by predictive analytics, which plays a pivotal role in identifying and preventing potential illegal trades before they materialize. Addressing the illicit supply and distribution of synthetic opioids can be encapsulated through these key points:

- **Actionable Intelligence**: Transform analyzed data into actionable intelligence, providing insights into the operations of illicit networks, targeting threat actors, illuminating threat networks, facilitating digital

underground undercover operations, and enabling specific selector leads that result into actionable intelligence to achieve information advantage. This information should be shared with LEAs for operational planning—including raids, arrests, and interdictions—to encourage a collaborative effort in this battle against drug trafficking.

- **Information Collection:** Deploy specialized software tools and trained personnel to access and navigate encrypted networks and hidden services on the dark web. Gathered data should be related to the sale, distribution, and logistics of fentanyl precursors, focusing on vendor profiles, buyer interactions, and transaction details.

    - Specialized units in these agencies must focus on digital forensics and cyber monitoring, thus equipping them with the necessary tools and knowledge to combat the digital aspect of drug trade and trafficking.

- **Data Analysis:** Process and analyze data collected from the dark web using advanced data analysis techniques—including AI and ML—to identify patterns and connections that indicate the operation of networks involved in the precursor chemical value chain.

- **Monitoring and Surveillance:** Establish a systematic and standardized approach to monitoring protocols related to fentanyl precursor chemicals and their emerging trends, especially utilizing novel, high-frequency, real-time systems. These findings can be used to gain a more nuanced and timely understanding of the tactics used by traffickers, which is crucial in preempting illegal activities and formulating rapid response strategies.

- **Threat Assessments:** Collect and evaluate data to identify threats and the impact these threats have on the current threat landscape posed by the proliferation of the fentanyl epidemic. These assessments should include the identification of threat actors and their networks, a review and analysis of their methods, tools, supply chains and tactics, and recommendations for the prioritization of threats emerging from the identified risks based on severity, credibility and potential impacts to the problem set.

- **Anonymity and Privacy Challenges:** Ensure the methods used for dark web intelligence collection and surveillance comply with applicable privacy, legal, and ethical frameworks and standards while effectively curbing fentanyl related dark web illegal activities.

Through this multi-pronged approach that encompasses physical and digital realms, LEAs can significantly reduce the illegal supply and distribution of synthetic opioids. This strategy not only targets the immediate issue of drug trafficking but also sets the foundation for a more resilient and adaptive response to future challenges in drug enforcement and public health policy.

A comprehensive strategy will further define requirements and support the selection of capabilities that integrate the appropriate authorities of all potential domestic and foreign stakeholders. CACI solutions applied to the fentanyl pathway defeat strategy will improve results-based outcomes for the counter-fentanyl mission.

ACTIONABLE INTELLIGENCE FROM THE DARK WEB

Dark web intelligence as an operational approach represents an increasingly important and sophisticated domain

within the broader field of intelligence gathering for the illicit drug trade. In particular, the dark web serves as a concealed part of the internet where illegal activities—from the sale of narcotics, weapons, and stolen data to the facilitation of various forms of cybercrime—can flourish with a higher degree of anonymity. To combat the fentanyl drug trade, leveraging dark web intelligence is crucial due to the widespread availability of fentanyl as a "research product" on the dark web.

Evolution and Current State

- **Early Awareness:** The intelligence community and LEA professionals have been aware of and engaging with the dark web for quite some time. Initially, the focus was primarily on monitoring and disrupting illegal marketplaces and forums where cybercriminals and other illicit actors operated.

- **Growing Sophistication:** Over time, the methods for collecting and analyzing data from the dark web have become more sophisticated. Techniques such as web crawling, automated data collection, and advanced analytics have been developed and refined to extract actionable intelligence from the dark web's vast and chaotic and often volatile dataset.

- **Integration with Mainstream Intelligence:** Dark web intelligence has become an integral part of cyber threat intelligence (CTI) operations for many organizations, both in the private sector and within government agencies. It complements other intelligence sources by providing insights into the motivations, tactics, techniques, and procedures (TTPs) of threat actors that might not be visible through surface web sources alone.

Additionally, the increased focus on combatting the illegal trade on the surface web creates the conditions for the observable shift in fentanyl precursors trade onto the dark web, as previously noted with other forms of illicit goods and services such as traditional drugs, firearms, and child sexual abuse material (CSAM).

Policymakers have established recommendations to guide the implementation of techniques that counter the rise of dark web-enabled drug shipments and precursor chemicals in the fight against drugs and crypto markets. Although Tor provides anonymity for buyers and sellers on darknet marketplaces, research has shown that data pulled from these marketplaces can be used to successfully identify criminal suspects who sell illegal narcotics and trade other illicit items to interested consumers. [xxxv] Furthermore, these sites are an exemplary case of problematic areas of information protection, prompting the need for specific practices when gathering data from the dark web.

The use of the dark web as an information source creates a challenge to the incumbent paradigm as relationships between drugs, sellers, and users are reconfigured online. [xxxvi] Understanding the internal structure of the dark web is essential for monitoring the activities executed on it. Criminals commonly exploit dark web forums to trade confidential information and illicit products. [xxxvii]

However, a lack of understanding about the nature of the dark web and criminals' utilization of it persists as a key challenge. [xxxviii] With the emergence of increasingly privacy-focused cryptocurrency markets on the dark web, the barriers to anonymously selling and procuring illicit goods and services diminish, posing a new set of challenges for law enforcement. When crime moves online, agencies need to be able to follow leads and conduct investigations seamlessly between the physical and digital worlds. [xxxix]

The illegal fentanyl trade has shifted from criminal networks to legally registered companies in China for production

and distribution, posing significant challenges for law enforcement and drug governance. Unregulated producers and vendors in China have been supplying fentanyl to North America, highlighting the necessity for global legislative regulation to effectively address the crisis. Moreover, the derivative effect of the Coronavirus (COVID-19) pandemic has impacted drug use behaviors, fentanyl exposure, and harm reduction service support among people who use drugs, further exacerbating the fentanyl crisis.

The evolving regulatory landscape for fentanyl requires a comprehensive approach that addresses the supply chain, trafficking trends, and the development of new high-intensity drug trafficking areas. Additionally, the presence of fentanyl in the illegal market, whether sold as such or disguised as other drugs, underscores the importance of increasing knowledge to reduce overdose risks among people who inject drugs.

As with any other commodity, LEAs must track the supply chain associated with all opioid variants. This process presents numerous potentially exploitable opportunities for U.S. law enforcement within a strategy aimed at disrupting pathways. Analysts can pinpoint potential actions and the most influential nodes impacting the synthetic opioid crisis by dissecting various components of the supply chain.

This includes precursors, laboratories, shipping methods, legitimate and illegitimate businesses, value transfer methods (currency and commodity), and individuals associated with the synthetic opioid trade. They can then utilize tools such as CARVER (Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability) analysis to extract valuable analytical insights from identified nodes.

In various steps of this process, unique data, the technology to collect such data and the expertise to analyze and extract value from such data will be required to highlight and disseminate actionable intelligence like portions of the value chain—such as open-source, business intelligence, social media, and deep and dark web data—to augment government data sources. While stepping through the value chain analysis methodology, gaps in authorities, resources, and data will likely be identified, which can undermine our chances of neutralizing the threat.

DarkBlue Intelligence Suite Tools and Services

A crucial aspect of addressing the fentanyl crisis involves highlighting supply chains, cargo trade routes, raw materials, and manufacturing equipment. Additionally, it involves focusing on finished fentanyl, especially by extending the scope of data collection, analysis, and dissemination. This extension should go beyond traditional intelligence methods, particularly in ungoverned digital spaces such as the deep and dark web.

CACI is well-versed in identifying gaps and developing solutions, including assisting in drafting new authorities, acquiring data, and identifying potential resources that can augment government data sources. Our researchers have employed proprietary tools, analytical methods, and expertise to identify, disrupt, and neutralize fentanyl distribution networks across these ungoverned digital spaces domestically and internationally. We have designed our capabilities to align with mission-critical needs and for tactical and strategic impacts, enhancing the ability to address this complex challenge.

DARKBLUE

DarkBlue is a software-as-a-service (SaaS) platform that revolutionizes how analysts tackle drug-related investigations on the open, deep, and dark web, offering the ability to exploit dark web intelligence and fentanyl related dark web activities. DarkBlue helps to skip the learning curve traditionally associated with dark web intelligence investigations by enabling practitioners to conduct research and link clues from multiple domains in one place. Our solution provides access to intelligence data from darknet markets, encrypted platforms, and channels, and through on-demand and tailored collection of clear net sites. It features advanced search and filtering options alongside top analytical tools, all integrated into an intuitive user interface (UI) enhanced with AI and ML capabilities.

DARKPURSUIT

DarkPursuit is an ephemeral browser-based single-session OSINT tool that ensures local browser information is never passed onto adversaries when conducting active dark web exploitation operations. Users can exploit fentanyl based dark web activities and pivot from analysis and targeting to secure browsing on the open web and popular darknets such as Tor, I2P, and Hyphanet (previously Freenet) in a reduced attribution capacity and collect and save page content and history to view them in DarkBlue. When users harness its extract, transform, and load (ETL) tooling to enhance and reveal site data, they can deanonymize site administrators on the open and dark web using open ports and IP addresses, gaining insightful and actionable intelligence against threat actors using the dark web to enable illicit drug trade pathways.

TECHNOLOGY-ENABLED ANALYST SERVICES

CACI employs technology-enabled analysts who are public trust and DOD-cleared, specializing in open-source intelligence (OSINT) and dark web intelligence. Their skills include monitoring, collecting, analyzing, and interpreting data from the open, deep, and dark web using operational analytical tradecraft, cyber threat intelligence, and dark web threat finance. Our analysts pursue fentanyl-related dark web activities and data on illegal goods and services, threat actors, and supply chains across the globe, utilizing specialized collection methods and software with AI and ML capabilities. Employing tools like DarkBlue and DarkPursuit for tailored cyber reconnaissance, they operate within darknets like Tor, I2P, ZeroNet, and Hyphanet (previously Freenet), encrypted channels like Telegram, and various social media platforms. Reports from CACI analysts offer invaluable threat intelligence into OSINT, the dark web, and other ungoverned digital live operating environments while staying current on the latest cyber technologies offering a comprehensive understanding of the constantly evolving threat landscape.

About CACI’s DarkBlue Intelligence Suite

CACI is a leader in open, deep, dark web access, exploitation, and analysis. Our powerful yet easy-to-use DarkBlue Intelligence Suite revolutionizes how OSINT analysts uncover the insights that accelerate their mission. With an easy integration between data exploration and collection, our tools, training, and expertise will help you securely discover, pursue, and engage without revealing your identity to adversaries or exposing your equipment to malware. To learn more, visit www.caci.com/darkblue.

References

The following United Nations fentanyl data sources references were used in this white paper:

- **UNODC site:** https://dataunodc.un.org/
- **Individual Drug Seizures (IDS) data collection:** https://dmp.unodc.org/downloadIDS
- **UNODC and illicit crop monitoring:** https://www.unodc.org/unodc/en/crop-monitoring/index.html
- **Statistical Annex:** https://www.unodc.org/unodc/en/data-and-analysis/wdr2023_annex.html

---

[i] https://www.dni.gov/files/ODNI/documents/IC_OSINT_Strategy.pdf

[ii] https://www.odni.gov/files/ODNI/documents/National_Intelligence_Strategy_2023.pdf

[iii] https://usafacts.org/articles/are-fentanyl-overdose-deaths-rising-in-the-us/

[iv] https://www.murphy.senate.gov/newsroom/in-the-news/fentanyl-is-single-greatest-challenge-us-faces-dhs-secretary-says

[v] https://www.cdc.gov/nchs/nvss/vsrr/drug-overdose-data.htm

[vi] https://www.cdc.gov/nchs/nvss/vsrr/drug-overdose-data.htm

[vii] https://www.murphy.senate.gov/newsroom/in-the-news/fentanyl-is-single-greatest-challenge-us-faces-dhs-secretary-says

[viii] https://home.treasury.gov/news/press-releases/jy1779

[ix] https://home.treasury.gov/news/press-releases/jy1413

[x] https://www.unodc.org/LSS/Announcement/Details/b152bda5-5d71-4f7e-9d68-1bdd9af04a83

[xi] https://home.treasury.gov/news/press-releases/jy1413

[xii] https://www.unodc.org/LSS/announcement/Details/f2adea68-fbed-4292-a4cc-63771c943318

[xiii] https://resources.darkblueintel.com/intel-reports/china-based-pharmacy-group-offering-xylazine-on-the-dark-web

[xiv] https://www.dea.gov/documents/2020/2020-03/2020-03-06/fentanyl-flow-united-states

[xv] https://www.justice.gov/opa/pr/largest-international-operation-against-darknet-trafficking-fentanyl-and-opioids-results

[xvi] https://dig.watch/updates/dark-web-marketplace-monopoly-market-seized-resulting-in-288-arrests

[xvii] https://www.europol.europa.eu/media-press/newsroom/news/darkmarket-worlds-largest-illegal-dark-web-marketplace-taken-down

[xviii] https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

[xix] https://www.techspot.com/news/88270-international-operation-brings-down-dark-web-largest-marketplace.html

[xx] https://twitter.com/TheJusticeDept/status/1308401473471078400

[xxi] https://www.fbi.gov/news/press-releases/JCODE-announces-61-arrests-in-its-second-coordinated-law-enforcement-operation-targeting-opioid-trafficking-on-the-darknet

[xxii] https://www.europol.europa.eu/media-press/newsroom/news/global-law-enforcement-action-against-vendors-and-buyers-dark-web

[xxiii] https://www.fbi.gov/news/stories/operation-disarray-040318

[xxiv] https://www.fbi.gov/news/stories/operation-disarray-040318

[xxv] Reuter, P., Pardo, B. and Taylor, J., 2021, "Imagining a fentanyl future: Some consequences of synthetic opioids replacing heroin", International Journal of Drug Policy, 94, p.103086. https://pubmed.ncbi.nlm.nih.gov/33423915/

[xxvi] https://www.dea.gov/sites/default/files/2021-02/DIR-008-21%202020%20National%20Drug%20Threat%20Assessment_WEB.pdf

[xxvii] https://www.unodc.org/res/WDR-2023/WDR23_B3_CH1_Synthetic_drugs.pdf

[xxviii] https://dmp.unodc.org/downloadIDS

[xxix] https://dmp.unodc.org/downloadIDS

[xxx] https://dmp.unodc.org/downloadIDS

[xxxi] https://www.unodc.org/res/WDR-2023/WDR23_B3_CH1_Synthetic_drugs.pdf

[xxxii] https://www.rand.org/content/dam/rand/pubs/research_reports/RR2700/RR2704/RAND_RR2704.pdf

[xxxiii] https://www.mitre.org/sites/default/files/2024-02/PR-24-0041-accelerating-the-fight-against-the-us-fentanyl-crisis.pdf

[xxxiv] https://dataunodc.un.org/

[xxxv] https://www.mdpi.com/2078-2489/9/8/186

[xxxvi] https://www.rand.org/content/dam/rand/pubs/research_reports/RR2700/RR2704/RAND_RR2704.pdf

[xxxvii] https://www.gao.gov/assets/gao-22-105101.pdf

[xxxviii] https://www.rand.org/content/dam/rand/pubs/research_reports/RR2700/RR2704/RAND_RR2704.pdf

[xxxix] https://www.rand.org/content/dam/rand/pubs/research_reports/RR2700/RR2704/RAND_RR2704.pdf