ISSN 2054-1910

GDPO Global Drug Policy Observatory
reporting monitoring analysis

MANCHESTER 1824 The University of Manchester

Swansea University Prifysgol Abertawe

Drug Cryptomarkets in the 2020s: Policy, Enforcement, Harm, and Resilience

Martin Horton-Eddison [*], Patrick Shortis [a], Judith Aldridge [¥], Fernando Caudevilla [p]

Policy Brief 16, June 2021

KEY POINTS

- Despite repeated recommendations from the UN General Assembly and several UN subsidiary bodies since 2013, there remains an absence of a single UN cybercrime convention, with *specific provision* for the illegal trade in drugs online.
- In this absence – and a decade after the founding of the original drug cryptomarket (Silk Road) - the standard and longstanding strategic enforcement model of 'takedown' endures.
- Evidence suggests that takedown is ineffective at reducing the size or scope of the illicit trade, increases market proliferation, and catalyses wide-spread market innovation, adaptation, and target hardening across the environment. This increases resource requirements exponentially, with ever-decreasing returns.
- It is likely that the current rate of technological evolution will create a shift to market types that lack some of the harm-reducing benefits of cryptomarkets, and that are more resource-intensive for law enforcement to monitor.
- New market types - encrypted apps or other peer-to-peer market platforms - lack some of the beneficial features that cryptomarkets provide over offline markets, reducing opportunities for harm reduction advice to reach users effectively. They may also increase the complexity of the response required (and the ability) of law enforcement agencies to curtail injurious elements of the online trade.
- Policies that encourage a nuanced enforcement approach – away from blanket takedown - might more efficiently focus limited human and financial resources only on the most injurious of substances and markets, freeing skilled cybercrime specialists to prioritise more pernicious criminal activities online, such as terrorism and child sexual exploitation.
- Such a guided approach might also ameliorate the negative consequences of takedown operations for ongoing harm reduction efforts, including for substance testing services that rely on drug cryptomarkets as conduits through which to communicate life-saving information.

[*] Dr. Martin Horton-Eddison is a Lecturer in International Relations at Cardiff University, and Research Officer at the Global Drug Policy Observatory with responsibility for its Drug Cryptomarket research project.

[a] Patrick Shortis is a PhD Candidate in Criminology at the University of Manchester and is the author of numerous GDPO publications on drug cryptomarkets.

[¥] Professor Judith Aldridge is a Professor of Criminology at the University of Manchester, UK.

[p] Dr. Fernando Caudevilla, Energy Control: AKA Silk Road's 'Doctor X' is an experienced medical doctor, Dr. Caudevilla is committed to reducing the harms associated with consumption. He oversees Energy Control's testing of samples purchased on drug cryptomarkets, totalling over 5,000 samples including cocaine, NPS, and MDMA (and more) purchased online since 2014, permitting people to discard or reject unsafe or unwanted substances.

INTRODUCTION

This GDPO Policy Brief is intended to inform policy-makers, practitioners, and other actors of the latest developments – and likely future direction – of Drug Cryptomarkets (DCM). It draws together several complementary active research strands to provide a timely trend analysis of the current and future state of the DCM landscape, clarifies the impact of a decade of counter-DCM policy and enforcement strategy on market development, and proposes suggestions for future enforcement strategies and wider policy guidance for the coming decade. We begin by detailing the history of counter-DCM operations to illustrate current and historic methods of enforcement. The brief identifies several likely future market innovations and trends for the coming decade. We then analyse the consequences of takedown on efforts to reduce some of the harms associated with DCM use, exemplified by the experiences of a high-profile drug checking service[1] located at the nexus of DCMs and harm reduction efforts. Finally, the brief presents a number of suggestions for policy-makers and enforcement practitioners. These include improving formal policy guidance to inform an adapted enforcement approach that prioritises targeting only the most injurious of vendors and markets, slowing the rate of innovation attrition, improving enforcement efficacy, and supporting ongoing harm reduction efforts.

TAKEDOWN: POLICY, AND ENFORCEMENT

The first law enforcement 'takedown' of an internet drugs market occurred in mid-1999, after US authorities noted an increase in smuggling by mail of significant quantities of controlled pharmaceuticals including alprazolam, diazepam, and codeine from Thailand. Investigations exposed three separate Thai-based vendor operators who were advertising substances on the internet in contravention of Article 3 of the 1988 convention and Article 10 of the 1971 convention.[2] Enforcement moved quickly: administrators were arrested, and servers unplugged. Over a decade after the Thailand takedown, the advent of drug cryptomarkets in 2011 represented a step-change in drug market innovation. Having evolved since the Thai operation, cryptomarkets are built on three core technologies; anonymising internet technologies including the onion router (TOR) or i2p to enable anonymous browsing and hosting, cryptocurrencies to enable 'digital cash' transactions, and escrow payment systems to facilitate trust in anonymous financial transactions by protecting buyers and vendors.[3] A decade after the founding (2011) - and 8 years since the takedown by law enforcement - of the original DCM (Silk Road) (2013), cryptomarkets now represent an established and maturing issue area for international drug control. Yet, despite the longevity and resilience of DCMs, enforcement practices nevertheless remain both rooted in the takedown principle first evidenced in the Thai operation and underpinned by international conventions that pre-date the advent of the internet itself.

"After we took down Hansa and Alphabay [in July 2017], we conducted a study on the type of impact the takedown provided and we realised that indeed it had a short life in terms of significant impact"

- EUROPOL Delegate, Remarks made to the Plenary, 61st CND 4th Intersessional, October 2018, Vienna, 23rd October 2018

Moreover, despite more recent high-profile (and increasingly sophisticated) law enforcement actions, DCMs nevertheless continue to function in 2021, and look set to continue operations – albeit in altering form - into the next decade. Indeed, 2020 data suggest[4] that purchases of drugs on cryptomarkets

continue to grow in Europe both before, during, and after the SARS-CoV-2 pandemic. The majority of substances bought and sold on these markets are typically described as 'recreational'[5] with cannabis by far the most commonly traded substance.[6] However the markets are also involved in the supply of synthetic opioids – specifically fentanyl and fentanyl analogues – substances implicated in compounding the (predominantly) United States' ongoing opioid crisis.[7]

At the international level, despite repeated official calls that 'something must be done' about DCMs - a comprehensive codified international approach nevertheless remains elusive. The United Nations Office on Drugs and Crime's (UNODC's) own 2013[8] call[9] for a dedicated international cybercrime instrument is yet to bear fruit, despite recent moves under the mandate of General Assembly resolution 74/247. Instead, limited DCM policy guidance is distributed in snippets across several disparate United Nations (UN) resolutions and statements. These are largely generalist in nature; the Commission on Narcotic Drugs' (CND) *Resolution 50/11* Paragraph 5 (2007) simply requests that member states provide 'assistance and equipment in support of both the International Narcotics Control Board (INCB) and UNODC's efforts'[10] against online sales. Over a decade since resolution 50/11– and in similar language - the INCB's Recommendations to Governments (2018) suggests that states should provide 'details from online sales, suspicious shipments, drug or illicit laboratory seizures.'[11] That same year, then UNODC executive director Yuri Fedotov pressed the 'importance of coordinated'[12] international police operations to address the issue. However, as recently as 2018 EUROPOL's Internet Organised Crime Threat Assessment (IOCTA) continued to decry the lack of a credible 'international strategy to address the abuse of the dark web.'[13] Recent work under General Assembly resolution 74/247 show little evidence of any attempt to incorporate specific DCM guidance. More broadly, to illustrate how little progress has been made since Resolution 50/11 (2007), the head of the UN agency tasked with combatting the use of cryptocurrency for money laundering – the GPML[14] - acknowledged that coordination and collaboration does not even occur between the GPML and the INCB - despite both bodies being located on the same floor of the same building in Vienna.[15]

Given the absence (at the time of writing) of a formal codified cyber-crime agreement - and in the face of disparate and generalist international guidance - it is hardly surprising that coordination of enforcement is both ad-hoc and sporadic. When coordination between national and international enforcement does occur, it is directed not by top-down international policy guidance, but by bottom-up enforcement practices. In effect, the result is enforcement-led policy, rather than policy-led enforcement.

In this vacuum, domestic and international law enforcement have defaulted to their stock trade of busts and seizures. Consequently, counter-DCM operations appear as *reactive* market takedowns; DCMs are typically removed by means of server seizure and the apprehension of administration staff in the same way as they have been since the Thai operation in 1999, the Silk Road operation in 2013, the takedown of 9 DCMs in 2014, and subsequent operations discussed in this brief. At their core, takedown strategies represent a 'one shot deal' that rarely considers the medium- to long-term consequences of market removal. Medium-to long-term consequences may be better understood if directed by a more comprehensive international position; one that accounts for a need to achieve the highest attainable standard of health, for which states and the international community have primary responsibility.[16]

CONSEQUENCES OF TAKEDOWN OPERATIONS

Aside from the immediate closure of a specific market, known consequences of takedown include accelerating market proliferation, impelling the development of technologies designed to evade detection by law enforcement,[17] galvanising long-term impact on cryptomarket activity,[18] and removing sources of live data for trend and substance analysis at all levels.[19] Market takedowns also significantly impede previously successful efforts to effectively reduce some of the harms associated with illegal drug consumption[20] including disconnecting communication channels between those monitoring substances and the buyers and vendors who trade in them.

Impact on Sales

Research shows that takedowns have a short-term impact because users simply migrate to other platforms to continue trading. Measuring overall trade volume on cryptomarkets by the feedback left by customers[21] evidences that following the takedown of the Silk Road, sales volume across DCMs returned to a pre-bust level within four months.[22] After the 2014 closure of multiple markets in Operation Onymous, the number of feedbacks left on markets exceeded pre-bust levels within two months.[23] Whilst the 2017 operation to close both Alphabay and Hansa Market may have been technically and tactically sophisticated, the impacts were again short-lived; evidence shows that overall trade volume across cryptomarkets recovered within a month of the Alphabay closure, and in a matter of weeks after the Hansa Market closure.[24] In short, markets and users seem to be recovering faster from disturbances caused by law enforcement operations and cryptomarkets continue to grow in number and patronage.

Target Hardening

Law enforcement efforts to suppress conventional drug markets has long been shown to result in so-called 'target hardening' by market actors, spurring marketplace innovation aimed at reducing the vulnerability of drug suppliers to detection and arrest.[25] We have seen substantial innovation in cryptomarket structures, security innovations and practices following law enforcement operations. One empirical study[26] showed how the FBI's seizure of the original Silk Road market helped accelerate the adoption of innovative multi-signature escrow technologies in replacement markets. This might usefully be described as an 'enforcement-innovation paradox', where each enforcement activity increases the level of resources and skills required to prosecute the next. Moreover, even though the lifespan of individual cryptomarket platforms is often short-lived, the entire ecosystem has tended to be highly resilient to law enforcement seizures of marketplaces, displacing vendors to alternative markets after which time sales again grow.[27] This "hydra effect"[28] is similar in conception to market fragmentation following enforcement activities against offline supply.

TECHNOLOGICAL INNOVATION – FUTURE TRENDS FOR THE 2020S

At present, cryptomarkets continue to respond to improvements in law enforcement investigative capacity by developing tradecraft and new market features. Continued destabilisation of cryptomarket platforms could ultimately result in wholesale shifts towards new market types such as encrypted apps or other peer-to-peer (P2P) market platforms. These emerging platforms lack many or all of the third party services provided by existing cryptomarket platform types, specifically; collated seller reliability metrics, escrow payment protection, centralised administration. As such, they provide fewer opportunities for harm reduction advice to reach users effectively, and curtail law enforcement's ability to engage in enforcement activities. Although some significant migration in this regard has already been observed, this is not yet at a point where a wholesale shift away from TOR has happened. It is our evidenced-based view that continued reliance on taking down markets will accelerate migration to emerging platforms.

"Since the suspect used a combination of Tor and [Monero], we could not trace the funds. We could not trace the IP-addresses. Which means, we hit the end of the road. Whatever happened on the Bitcoin blockchain was visible and that's why we were able to get reasonably far. But with Monero blockchain, that was the point where the investigation has ended".

– Europol Analyst Jarek Jakubchek - Blockchain Alliance Webinar on Privacy Coins, December 10, 2019

In a similar vein, recent shifts in tradecraft as a response to enforcement activity already include improvements in Bitcoin privacy and the widespread adoption of Monero,[29] which severely limits the capacity of law enforcement to reveal buyer and seller identities via blockchain analysis.[30] Whilst Bitcoin continues to be the most popular cryptocurrency, the relative ease with which it can be deanonymized through blockchain analysis has led to the development of mixing protocol technologies like CoinJoin[31] and Wasabi[32] wallet. These technologies enhance Bitcoin privacy by mixing the transactions of multiple users together to obfuscate identities, use TOR to obfuscate traffic, and are reportedly creating challenges for blockchain analysis companies and law enforcement investigations.[33] Monero - a more anonymous alternative to Bitcoin - and one that has stymied several law enforcement investigations - is now widely adopted across most cryptomarkets, with an increasing number actively encouraging its use over Bitcoin.[34]

In tandem with an effort to deny law enforcement investigatory leads through blockchain analysis, market staff have also learnt that digital traces left on markets pose threats for all users, and are attempting to reduce those traces and improve security. Current market leader (Feb 2021) White House Market uses Monero as its primary payment method *and* forces the use of pretty good privacy (PGP) encryption for all activities including orders and messages, with the purpose of denying law enforcement access to these sources of information in the event of a market seizure[35]. For example, Monopoly market launched as a Monero-only market with a new order process that signals a shift towards *de facto* decentralisation: Instead of creating accounts to purchase from, customers make orders directly from vendors and are given an order number they can use to track the progress of their purchase. The market allows for optional payment by escrow, but the system encourages direct dealing, with the market collecting monthly fees from its pre-vetted vendors. Therefore, in the event of market seizure by law enforcement, no customer order data will be available to law enforcement agencies. In this way, Monopoly is marginally more decentralised than some of its peer markets, with the administrator playing less of a direct role in the purchasing process. Whilst this innovation protects customer data, it also removes a communication channel between the administrator and customers; buyers do not have an account inbox that they can receive messages (including harm reduction announcements) through.

Both *White House* and *Monopoly* markets issue rigorous guides on reducing the risk of engaging in the cryptomarket trade, including detailed instructions for improving user operational security practices. In the face of law enforcement takedown operations, platform administrators and staff have responded by improving the security behaviours of their users to lower the likelihood of apprehension. This sort of innovation is critical in a context where arrests are enabled by mistakes on the part of users that leave digital evidence trails. To illustrate; the seizure of *Wall Street Market* in 2019 precipitated the arrest of 179 vendors around the world. The operation used data gleaned from the seizure of the market's servers including unencrypted messages between vendors and customers

that contained users' physical addresses and the digital addresses of their bitcoin wallets.[36] Accordingly, if cryptomarket administrators continue to work diligently to enforce Monero adoption and PGP encryption than we can expect future market takedowns to net diminishing intelligence returns.

More broadly, the threat of law enforcement coupled with the onslaught of distributed-denial-of-service (DDOS) attacks over the last year[37] have had a galvanising effect on innovation in cryptomarkets. Combined, they may partially account for a slow but growing shift to peer-to-peer (P2P) market platforms. For several years, researchers and cryptomarket watchers have voiced concerns about cryptomarket drug transactions moving from centralised cryptomarkets to decentralised P2P trade platforms like OpenBazaar or selling over chat applications such as Wickr and Telegram. Decentralized markets remove some of the positive aspects of cryptomarkets that customers enjoy and are harder for law enforcement agencies to police.[38] At present cryptomarkets are centralised platforms that provide third party services in return for a commission on sales. By contrast, in a decentralised model each vendor has full control over all aspects of trade. Without centralised control over the systems for payments, disputes and reviews, and an active discussion forum space, the incentives for vendors to be honest about the quality and consistency of their products are reduced without independently verified customer feedback or the threat of being removed from the platform.

In spite of the comparative disadvantage of decentralised platforms for drug trading by comparison to cryptomarkets, over the past two years we have witnessed a slow trickle of users to encrypted chat platforms like Wickr for direct dealing with vendors. Some users move to Wickr because of the increasingly complex nature of DCMs as a barrier to access.[39]. With the recent launch of Televend - a Telegram-based autoshop system we may find even more buyers and sellers considering taking their chances with direct dealing.[40] Televend, whilst still to some degree centralised in its infrastructure, fees and review system, is likely to become an increasingly attractive option due to reduced market downtimes. It may also pose new problems for police investigations, including the inability to takedown the server without also removing the Telegram app: Law enforcement agencies should therefore consider carefully what kind of enforcement strategies they employ.

ROLE OF DRUG CRYPTOMARKETS IN REDUCING HARMS

Research suggests that some of the harms of drug use that are created by prohibition may to an extent be reduced by the cryptomarket drug trade.[41] Customer feedback metrics and escrow payment protection combine to encourage and reward vendor accountability. Compared to offline drug buyers therefore, cryptomarket buyers may be more likely to obtain a higher quality and 'as advertised' products. This is important because some drug harms arise from uncertain content and strength, thereby creating the risk of unwanted effects or overdose. Cryptomarket vendors often provide warnings associated with high-purity products, allowing users to make better-informed decisions about product choice and dosage, and may therefore function to reduce harms associated with accessing products in offline drug markets.

In addition, cryptomarket discussion forums have provided a rich source of drug safety information (e.g., quality, purity, adulterants, dosing), enabling buyers and vendors alike to share information about product and batch content, and about buying and selling more safely. This kind of information is not typically available on popular and reputable drug-safety forums on the clearnet (e.g., Bluelight.org), as these sites usually have policies that explicitly ban discussion related to drug supply. Other

clearnet discussion locations (Reddit groups) have been closed following legal rulings in the US, making the existence and support of DCM forums even more important. The quality and accuracy of information generated in marketplace discussion forums is - of course - not guaranteed, and inaccurate information could potentially increase the risk of harmful outcomes. However, in cases of best practice cryptomarkets have facilitated discussion threads hosted by qualified drug harm reduction professionals, often resulting in high-quality drug safety information being made permanently archived for users.

Case Study: Active Harm Reduction Initiatives

As early as the first iteration of the Silk Road, Dr Fernando Caudevilla[42] (aka "Dr X") provided expert medical harm reduction advice to buyers and vendors on DCMs. Information was provided to drug users who sought advice they felt unable or unwilling to seek from offline or even clearnet medical professionals. Questions included how controlled substances might interact with prescribed substances, on how to manage adverse effects, psychiatric conditions, help with abuse or dependence, and advice to expectant or breastfeeding mothers. In the years immediately after the Silk Road takedown, users on replacement markets including Silk Road 2.0 and Evolution continued to seek advice, resulting in tens of thousands of views of medical advice posted in reply to specific questions on discussion forums.

Today, Dr Caudevilla works for Energy Control, an organisation that since 2014 has combined a comprehensive international drug checking service with expert medical harm-reduction information, personal medical advice and education to service users from around the world. Energy Control's drug checking service is well-used by those buying drugs through online markets. Energy Control provides colorimetric, thin layer chromatographic, and mass spectrophotometric testing to analyse content and purity of substances

See also:
Caudevilla, F., The emergence of deep web marketplaces: a health perspective. In European Monitoring Centre for Drugs and Drug Addiction (Ed.), The internet and drug markets (EMCDDA Insights 21) (pp. 69-75). Luxembourg: Publications Office of the EU., 2016

bought online. The results allow users to make informed choices to reject and dispose of contaminated or dangerous substances, helping to reduce risk, prevent overdose, and to minimise medical complications that may arise from use. Significantly, Energy Control's testing of samples acquired on drug cryptomarkets also feeds data into the UNODC's scientific research, providing valuable information for policy-makers and practitioners at all levels.

In operational terms, test results from cryptomarket drug purchases enable Energy Control to contact cryptomarket platform administrators to inform them of unexpected and potentially more dangerous substances being sold. Energy Control data has already identified suppliers of fentanyl-adulterated heroin samples and communicated those results through clear web and cryptomarket forums, resulting in listings being removed and vendors banned by market administrators. These positive harm-reducing initiatives are only possible because drug cryptomarkets exist in their well-known centralised form. When law enforcement closes marketplaces, gone too are the possibilities for providing tailored advice, test results, and safety information to people who use drugs: access to the vulnerable populations is stymied by takedowns. Moreover, whilst drug cryptomarkets remain centralised platforms managed by administrators, it is still possible to communicate directly with those capable of removing listings or vendor accounts. As

the ecosystem innovates to a decentralised model of peer-to-peer hosted vendor shops as discussed earlier (e.g., Televend), then providing information and having bad actors removed becomes less feasible, so reducing the efficacy of some valuable harm reduction-oriented initiatives.

Social Harms

Cryptomarkets may, additionally, reduce the likelihood of violence associated to the trade in illegal drugs[43]. Because transactions occur online, opportunities for violence will be substantially fewer than where transactions are face-to-face. Moreover, cryptomarket platform features, like escrow and dispute adjudication, may function to reduce the kinds of conflict that give rise to violence. Because cryptomarkets serve an – albeit limited – wholesale function,[44] violence reduction may also apply for the stock sourcing purchases where offline drug violence is more concentrated. However, as the number of market takedowns and arrests increase, trust in the cryptomarket eco-system may, in turn, be eroded, thereby impacting otherwise more peaceable trading, resulting in increased conflict and violence.

Self-Regulation

Cryptomarkets can be understood as platforms that function to regulate illicit drug trading by virtue of the third-party services (e.g., escrow, dispute adjudication) that mimic those available in legal markets. Since 2011, markets have been observed engaging in self-regulatory behaviours. Most notably, these include banning and vetting particular products and services.[45] Such initiatives are aimed not just at reducing trading disputes, but also at reducing wider drug harms by removing or banning specific substances known to be injurious to users. Indeed, Vince O'Brien of the UK National Crime Agency (NCA) noted that some vendors on DCMs appeared to be self-enforcing the broader international position on fentanyl, removing listings and banning vendors who flouted the rules.[46] Indeed, Dream Market self-regulated (removed) all product listings and proscribed fentanyl products alongside assassinations, child pornography, and weapons of mass destruction. However, a few DCMs continued to feature fentanyl products openly. Moreover, several markets – most notably the Russian-hosted Tochka Market - continued to list the substance for international delivery via major international postal carriers. O'Brien speculated that vendors and markets were voluntarily delisting fentanyl due to intense moral concerns about the proportionately high death rate. This may not be entirely altruistic behaviour; if law enforcement prioritise actions against vendors trading in particularly injurious substances, vendors and platforms supporting bans on these substances may be operating with self-interest. A 2021 Australian study found that law enforcement interventions that targeted specific substances – such as fentanyl – and only those markets implicated in their sale is a particularly effective approach.[47] Furthermore, recently evolved law enforcement strategies that first undermine trust in live DCMs (before ultimately taking them down) may also contribute to DCM self-regulation.

CONCLUSIONS AND RECOMMENDATIONS

Default takedown enforcement models closely resemble the decapitation strategies used throughout the 'war on drugs' in the offline world. Perhaps unsurprisingly, this has had similar effects online; the fragmentation of markets, acquisition of new skills and tools on behalf of traffickers, and the creation of markets that are increasingly driven by profit incentives fuelled by the consequential risk/reward quotient. More recent counter-darknet law enforcement operations – most notably Operations Gravesac and Bayonet[48] - have begun to accommodate changing enforcement practices, including undermining general trust in the markets, using the markets as live sources of intelligence, and even managing live DCMs as part of operations. Operations like these depend on centralised market designs with servers and administrators at the

helm. However, recent market innovations are accelerating technical change toward decentralisation. At the same time, cybercrime investigatory skills (and personnel) are also deployed against a range of online issues including countering child abuse, the trade in illegal firearms, fraud and money laundering, and terrorism activities. Finite enforcement resources are understandably stretched.

As such, enforcement practices logically require revision, but this is problematic in an enforcement-led policy environment devoid of codified international guidance. A cybercrime convention *with specific provision for drug cryptomarket* guidance would be a useful first step toward acknowledging the negative consequences of the existing approach. It might also see the online trade in drugs as part of a more holistic approach to cybercrime. One benefit might be that the cryptomarket drug trade is recognised as a lower-order priority – at both the international and enforcement level - compared to the online trade in child abuse material, terrorism, and the trade in weapons. However, to be successful, any formal agreement must recognise the harm-reducing realities of drug cryptomarkets and respond accordingly, although what this might look like in practice is less clear. One approach might be to prioritise enforcement against only those vendors and markets that permit the trade in particularly injurious substances including fentanyl and fentanyl analogues. De-prioritising the trade in recreational drugs would not only slow the rate of technological innovation in response to takedown operations, but also liberate cybercrime enforcement practitioners to focus skills, time, and financial resources on those more pernicious cybercrimes as described.

It is recognised that regulating the production, use, or trade in internationally controlled substances for non-medical and non-scientific purposes is neither within the spirit nor letter of the existing drug control conventions. That said, the protection of public health has always been a key overarching aim of the existing treaties, and of intersecting institutions. Any new cybercrime instrument – if inclusive of specific provision for drug cryptomarkets - and that interlocks with the existing prohibition-oriented architecture, might facilitate a targeted approach in accordance with a nuanced interpretation of the Single Convention's desire to protect the 'health and welfare of mankind.'[49] At present, despite UNODC's role[50] as the Secretariat for the ad hoc committee to elaborate a comprehensive international convention on countering cybercrime, there is little evidence of any intention to include specific provision for managing international responses to drug cryptomarkets.

Recommendations:

Inform enforcement practitioners of the risks associated with blanket takedown approaches

Target only vendors and markets that facilitate the distribution of the most injurious of substances

Recognise and prioritise harm reduction potential of markets

Leverage UNODC's unique position to ensure inclusion of specific provision for DCM policy - informed by diverse actors including enforcement, civil society, and academia - in any new cybercrime treaty

ACKNOWLEDGMENTS

The authors would like to thank Dave Bewley-Taylor, GDPO Director, for his editorial input, and especially Monica Barratt, National Drug and Alcohol Research Centre, University of New South Wales, for her invaluable peer review and insightful suggestions. Any errors of fact or interpretation remain with the authors.

ENDNOTES

1 *Drug Checking Services* facilitate members of the public to anonymously submit drug samples to receive individualised analysis and results. See, for example: Barratt, M.J., Kowalski, M., Maier, L.J., & Ritter, A., *Global Review of Drug Checking Service Operating in 2017*. Drug Policy Modelling Program Bulletin No. 24. Sydney, Australia: National Drug and Alcohol Research Centre, UNSW Sydney. 2018

2 E/INCB/2000/1, *Report of the International Narcotics Control Board for 2000*, INCB, Vienna, 2000. P.19, Para 100.

3 Horton-Eddison, M, *Updating Escrow; Demystifying the CDM Multisig Process*, GDPO, Swansea, June 2017

4 EMCDDA Special Report, *Covid19 and Drugs; Drug supply via darknet markets*, EMCDDA, Lisbon, May 2020. P.3

5 For example, heroin makes up 28% of the European drugs market but only 6% of the cryptomarket trade. See: Kruithof, K., Aldridge, J., Décary-Hétu, D., Sim, M., Dujso, E. & Hoorens, S., *Internet facilitated drugs trade. An analysis of the size, scope and the role of the Netherlands*, Santa Monica, RAND Europe, 2016

6 Christin, N & Thomas, J. *Analysis of the supply of drugs and new psychoactive substances by Europe-based vendors via darknet markets in 2017–18*, EMCDDA, Lisbon, 2019

7 Horton-Eddison, M, Response to Fentanyl Crisis Reflects Evolutions in Dark Web Policing, *Jane's Intelligence Review*, Vol.31, No. 2, February 2019. Pp. 46–9

8 UNODC, *Comprehensive Study on Cybercrime*, Draft, February 2013. P. xii

9 Recommended in Feb 2013 by the CCPCJ's Open-Ended Intergovernmental Expert Group (OEIEG) – itself established by Para 42 of the Salvador Declaration (April 2010) (UNIS/CP/614, CCPCJ) – see also E/CN/.15/2011/19, ECOSOC, CCPCJ 20th Session (background)

10 E/CN.7/2007/16, CND Resolution 50/11, 'International cooperation in preventing the illegal distribution of internationally controlled licit substances via the Internet', CND, Vienna, 2007. Para 5, P. 48

11 INCB, *INCB Report 2018*, Recommendations to Governments, the United Nations and other relevant international and national organizations, Chapter IV, Recommendation 22, P. 113

12 Fedotov, Yuri, Director General / Executive Director UNODC, *Remarks at the Launch of the World Drug report 2018*, New York, 26th June, 2018.

13 EUROPOL, *Internet Organised Crime Threat Assessment* (IOCTA) 2018, European Cybercrime Centre (EC3), European Union Agency for Law Enforcement Cooperation, 2018. P. 13

14 Global Programme against Money Laundering

15 Van Dyk, Michiel, Remarks made to the Plenary, 61st CND 4th Intersessional, October 2018, Recorded Participant Observation transcript, Vienna, 22nd October 2018

16 WHO, Constitution of the World Health Organisation, New York, 1946

17 Horton-Eddison, M. & Di Cristofaro, M., *Hard Interventions and Innovation in Drug Crypto-Markets: The Escrow Example*, GDPO Policy Brief 11, GDPO Swansea, August, 2017

18 Van Buskirk, J, Bruno, R., Dobbins, T., Breen, C., Burns, L., Naicker, S. & Roxburgh, A., The Recovery of Online Drug Markets Following Law Enforcement and Other Disruptions, *Drug and Alcohol Dependence*, Vol. 173, April 2017. Pp. 159–62

19 Aldridge, J., & Bouchard, M., Leveraging the value of online data and methods: Drug policy research at the cutting edge. *Int Journal of Drug Policy*, No.73, 2019, Pp. 208–09

20 Caudevilla, F., *The Emergence of Deep Web Marketplaces: A Health Perspective*, in: *The Internet and Drug Markets*, EMCDDA Insights, Iss. 21, Luxembourg, February 2016

21 Aldridge, J., & Décary-Hétu, D., *Not an 'Ebay for Drugs': The Cryptomarket "Silk Road" as a Paradigm Shifting Criminal Innovation*. 2014

22 Soska, K., & Christin, N. (2015*). Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem*. Paper presented at the USENIX Security '15, Washington DC.

23 Décary-Hétu, D., & Giommoni, L. *Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous*. Crime, Law and Social Change, 2016. Pp. 1–21

24 Dittus, M., *A distributed resilience among darknet markets?* [Online]. Oxford Internet Institute.

25 Bouchard, M. (2007). *On the resilience of illegal drug markets. Global Crime, 8*(4), 2017. Pp.325–44

26 Horton-Eddison, M. & Di Cristofaro, M., *Hard Interventions and Innovation in Drug Crypto-Markets: The Escrow Example*, GDPO Policy Brief 11, GDPO Swansea. August, 2017

27 See for example: Décary-Hétu & Giommoni, 2016; Soska & Christin, 2015; Van Buskirk et al., 2017

28 Maddox, A., *Disrupting the Ethnographic Imaginarium: Challenges of Immersion in the Silk Road Cryptomarket Community*, Journal of Digital Social Research. 2 (1) 2020.

29 MoneroHow. (2017*) How does Monero privacy work?* [Online]. Monero.how

30 Blockchain analysis is used by private actors and law enforcement agencies to deanonymize cryptocurrency transactions and link users to their real-world identities.

31 Maxwell, G., *CoinJoin: Bitcoin Privacy for the Real World* (Post on BitcoinTalk forum), 2013

32 WasabiWallet., *Wasabi Wallet: reclaim your privacy now* [Online], 2018

33 Southurst, J., *Europol report on Wasabi Wallet reveals law enforcement scrutiny*: CoinGeek, 2020.

34 Stevens, R. *Monero transactions untraceable, says Europol analyst* [Online]. Decrypt, 2020

35 WhiteHouseMarket. (2019) White House Market User Guide [Online]. White House Market.

36 This kind of data aids blockchain analysis techniques

37 Cimpanu, C., *Dark web crime markets targeted by recurring DDoS attacks* [Online]. ZDNet, 2019.

38 Buxton, J. & Bingham, T., *The Rise and Challenge of Dark Net Drug Markets*, Swansea: Global Drug Policy Observatory, 2015.

39 Moyle, L., Childs, A., Coomber, R., & Barratt, M. J., *#Drugsforsale: An Exploration of the Use of Social Media and Encrypted Messaging Apps to Supply and Access Drugs*. International Journal of Drug Policy, No.63, 2019. Pp.101–10

40 Power, M., *A New Robot Dealer Service Makes Buying Drugs Easier Than Ever*: Vice, 2020.

41 Aldridge, J., Stevens, A., & Barratt, M. J., *Will Growth in Cryptomarket Drug Buying Increase the Harms of Illicit Drugs?. Addiction*, 113(5), 2018. Pp. 789–96.

42 Dr. Fernando Caudevilla, Energy Control: AKA Silk Road's Doctor X. An experienced medical doctor, Dr. Caudevilla is committed to reducing the harms associated with consumption. He oversees Energy Control's testing of samples purchased on drug cryptomarkets, totalling over 5,000 samples including cocaine, NPS, and MDMA (and more) purchased online since 2014, permitting people to discard or reject unsafe or unwanted substances.

43 Barratt, M. J., Ferris, J. A., & Winstock, A. R., *Safer scoring? Cryptomarkets, social supply and drug market violence*. International Journal of Drug Policy, 35, 2016. Pp.24-31. AND Morselli, C., Décary-Hétu, D., Paquet-Clouston, M., & Aldridge, J., *Conflict Management in Illicit Drug Cryptomarkets*. International Criminal Justice Review, 27(4), 2017. Pp.237–54.

44 Aldridge, J., & Décary-Hétu, D., Not an *'Ebay for Drugs': The Cryptomarket "Silk Road" as a Paradigm Shifting Criminal Innovation*, 2014

45 Morselli, C., Décary-Hétu, D., Paquet-Clouston, M., & Aldridge, J. (2017). Conflict management in illicit drug cryptomarkets. International Criminal Justice Review, 27(4), 237–54.

46 Horton-Eddison, M, Response to Fentanyl Crisis Reflects Evolutions in Dark Web Policing, *Jane's Intelligence Review*, Vol.31, No. 2, February 2019. Pp. 46–9

47 Broadhurst, R., Ball, M., Jiang, C., Wang, J., Trivedi, H., *Impact of Darknet Market Seizures on Opioid Availability*, AIC Research Report 18, Serious and Organised Crime Laboratory, Australian Institute of Criminology, 2021. P.44

48 For more information on Gravesac and Bayonet see: Afilipoaie, A. & Shortis, P., *Cryptomarket Enforcement - New Strategy and Tactics*, GDPO Situation Analysis, Swansea, June 2018

49 United Nations Single Convention on Narcotic Drugs, UN, 1961, preamble.

50 Through the Organized Crime and Illicit Trafficking Branch of the Division for Treaty Affairs

supported by

About the Global Drug Policy Observatory

The Global Drug Policy Observatory aims to promote evidence and human rights based drug policy through the comprehensive and rigorous reporting, monitoring and analysis of policy developments at national and international levels. Acting as a platform from which to reach out to and engage with broad and diverse audiences, the initiative aims to help improve the sophistication and horizons of the current policy debate among the media and elite opinion formers as well as within law enforcement and policy making communities. The Observatory engages in a range of research activities that explore not only the dynamics and implications of existing and emerging policy issues, but also the processes behind policy shifts at various levels of governance.

Global Drug Policy Observatory
Research Institute for Arts and Humanities
Room 201 James Callaghan Building
Swansea University
Singleton Park, Swansea SA2 8PP
Tel: +44 (0)1792 604293
www.swansea.ac.uk/gdpo

@gdpo_swan