Evolving Reality: The Strategic Shift in Crypto-Drug Market Enforcement

Martin Horton-Eddison, Global Drug Policy Observatory

m.horton-eddison@swansea.ac.uk

Introduction

Crypto-Drug Markets (CDMs), also referred to as Dark Net Drug Markets are anonymised internet sites which facilitate the sale and purchase of narcotic substances both domestically and internationally.

This statement offers a strategic assessment of the evolving CDM Law Enforcement landscape, and some thoughts on the future direction of CDMs and CDM enforcement.

'Historic' Strategic Approach

In the recent past, the standard law enforcement strategy has been one of *site takedown*, aimed at arresting CDM administrators, and eliminating site servers with the sole purpose of taking the CDM offline. On the face of it, the site takedown strategy, as applied to the original Silk Road and its immediate successors, seemed a logical response – forcing sites simply to cease to exist.

Although CDMs represent a *novel* threat, *takedown* may be usefully described as *conventional*: utilising existing law enforcement force-structures, general agents and agencies, and often unilateral approaches in order to attack the CDMs' Centre of Gravity; to *takedown* the hub on which everything depends.

The Failure of Takedown Strategy

However, despite numerous high-profile historic takedowns, CDMs continue to exist – with new sites emerging or increasing their capacity to facilitate the online trade just as quickly as their predecessors can be taken down. To illustrate the point: the value of CDM drug transactions rose by 50% in the two years following the takedown of Silk Road in 2013. As can be seen by the slide, even by the UNODC's own assessment therefore, *takedown* simply doesn't appear to work.

Essential Trust

The survivability and continued proliferation of Crypto-Drug Markets appears to depend on assurance of several key *trust* areas: trust in the market , trust between vendors/buyers, trust in the payment systems and currency, trust in the assurance of anonymity , and trust in delivery services. The evidence indicates that takedown may provoke the adoption of new technologies, increase public awareness – and therefore usage - of CDMs, and does little to undermine trust in many of the specific areas mentioned.

Evolution

Since 2017, domestic and international law enforcement appear to be adapting their approach, moving toward enforcement strategies which prioritise less conventional means. Law enforcement

operations in 2017 and 2018 have displayed a more nuanced and sophisticated approach. Although operations are still managed by conventional law enforcement agencies, the strategic onus appears to be shifting toward the deployment of multiple specialist enforcement agencies, specialised agents, and complex joint international operations between multiple state partners. For example, the 2017 multilateral takedown of AlphaBay occurred only after law enforcement had taken control of Hansa Market as a honeypot – a tactical step ahead of the markets' users.

This evolved strategy more closely targets our earlier essential elements of trust in - and function of - CDMs:

Trust in the market – may be undermined if it is possible that the market is being operated by law enforcement

Trust between Vendors/Buyers – may be undermined if it is possible that either is a law enforcement agent

Trust in the payment systems and currency – may be undermined if currency exchanges might be being operated by law enforcement

Trust in Anonymity – may be undermined if law enforcement can infiltrate the site to access communications between buyer and vendor

Trust in delivery – may be undermined if postal services are working closely with law enforcement to intercept deliveries

Many of these elements are addressed by the evolving law enforcement strategy. The deployment of the United States Postal Inspection Service (USPIS) to intercept packages, the Netherlands' National High Tech Crime Unit (NHTCU) to actually operate live CDMs, US agents posing as money launderers for Bitcoin and other cryptocurrencies, and private companies such as Bitdefender providing unprecedented access to servers. Each provide clear examples of the strategic shift away from conventional takedown and toward an evolved approach. Strategically speaking, we might usefully characterise the increased involvement of ancillary agencies and the deployment of smaller specialised and more nimble teams with specialised roles as something akin to a form of counter insurgency operation – using small force units with specialist skills, embedded in the 'local population', and sanctioned by sophisticated international alliances.

A consequence of the evolved approach is that many of those points of trust as discussed earlier are more effectively undermined when compared to conventional takedown.

Concluding Remarks

In response to law enforcement operations and other factors, CDMs are technologically adaptive. Tomorrow's CDMs appear likely to be both decentralised – i.e having no central administration – and geographically distributed – with no central servers. These developments will render *takedown* completely obsolete. Law enforcement strategy will have to continue to innovate in order to keep pace with these developments, becoming increasingly more specialised, time consuming, and

expensive – in turn. There may therefore be a need to balance the increasing expenditure against likely harm – for example considering market management approaches over purely punitive enforcement – as we are increasingly seeing in offline policy shifts around the world. Efforts such as targeting only the most pernicious of vendors - rather than whole Crypto Drug Market sphere - may be one efficient strategy, allowing policy makers to more effectively balance the need to influence serious negative behaviour, with a nuanced awareness of the potential for CDMs to reduce both personal and social harm.