The Rise and Challenge of Dark Net Drug Markets

Julia Buxton* & Tim Bingham∞

Policy Brief 7 | January 2015

Key Points

- Recent years have seen a dramatic growth in the sale of a variety of illicit substances on Dark Net drug markets, with on line sales projected to increase exponentially due to expanding internet availability, evolving technologies and the profusion of social media.

- This new form of retail market poses a major challenge to not only law enforcement agencies but also the UN international drug control system and related legal structures within which these agencies operate.

- For vendors and purchasers who use the sophisticated, user friendly and increasingly secure Dark Net sites, hidden markets present a safer environment for drug transactions and they reduce the multiple risks (coercion, violence, arrest, exposure to other drugs) associated with 'street' sales.

- Research demonstrates that anonymised user forums and online chat rooms encourage and facilitate information sharing about drug purchases and drug effects, representing a novel form of harm reduction for drug users and an entry point for drug support services.

- Experience to date shows that enforcement efforts through surveillance, hacking and other forms of interdiction may be successful in closing down a particular site, but at the cost of proliferating hidden drug markets and incentivising technological innovation.

- Given an acknowledged lack of technical capacity, legal constraints and poor international enforcement coordination, Dark Net interdiction efforts should prioritise high-end crimes such as child sexual exploitation, cyber terrorism and weapons trafficking, and work with self-regulating, 'ethical' drug sites to enhance understanding of high-level criminality on the Dark Net.

- The 2016 UN General Assembly Session (UNGASS) on the World Drug Problem is a timely opportunity to discuss reform of the UN drug control treaty system to better deal with the challenges of the increasingly complex illicit drug market in the twenty-first century.

* Senior Research Officer, GDPO, Swansea University

∞ Independent researcher & Research Associate, GDPO, Swansea University

INTRODUCTION

This policy brief examines the expansion of drug markets on the Dark Net or 'hidden web' and the challenges they pose for both law enforcement agencies and the international legal framework within which those agencies ultimately operate. The Dark Net drug markets are one manifestation of an increasingly complex, transnationalised and lucrative trade that the extant United Nations drug control system, and the treaties upon which it is based, is poorly positioned to address. The 1961 Single Convention on Narcotic Drugs, the bedrock of the international drug control architecture, does much to lock the international community into arcane and bureaucratic counter-narcotic responses oriented toward criminalisation and law enforcement. However, evidence has demonstrated that this approach has failed to achieve a significant or sustainable reduction in drug supply or demand.[1] Conceived before the challenges of globalisation, transnational organised crime, HIV, and the electronic communications revolution, the drug treaty system and associated 'traditional' counter narcotics strategies are increasingly inadequate tools with which to address emerging challenges such as the Dark Net drug markets.

Within this context, this brief discusses the limitations of traditional law enforcement strategies in matching, let alone exceeding the sophistication and innovation of the hidden web and digital crypto-currencies used for payment on the Dark Net drug markets. Enforcement responses risk exacerbating rather than addressing the 'problem'. Efforts to intercept, disrupt and contain the hidden markets — as with all facets of drug trade interdiction – will likely serve only to diversify and professionalise these illicit interactions. The key recommendation of this brief is that rather than looking to improve enforcement capabilities such as interception and electronic surveillance, (and in a manner that increasingly encroaches on civil liberties), official responses should give primacy to understanding how 'ethical' hidden web drug markets that are regulated by their user communities and market forces might reduce the harms and violence of the 'traditional' drug trade and networks. This harm reduction approach would enable scarce cyber-crime resources to be dedicated to high-end abuse of the Dark Net, such as child sexual exploitation; networks for weapons trafficking, financial hacking and identity theft; and cyber-terrorism.[2]

Given projected growth of internet use beyond the current 2.8 billion, the sophistication and ease of encryption applications, and growing specialisation in online retail and distribution chains, the emergence and expansion of hidden drug markets reinforce the argument that dramatic change is required in the way drug control is conceptualised and enforced, and the importance of pragmatic, evidence based responses. As the United Nations Office on Drugs and Crime's (UNODC) 2014 *World Drug Report* sets out in its first ever mention of the phenomenon, the hidden Dark Net drugs markets have 'the potential to become a popular mode of trafficking in controlled substances in years to come.'[3] This necessitates radical and nuanced new approaches that minimise harm.[4] The hidden drug markets, like so many facets of today's smart, modern drug trade cannot be addressed through approaches devised half a century ago. Here we suggest that the United Nations General Assembly Special Session (UNGASS) on the World Drug Problem in 2016 is an ideal opportunity to engage in serious discussion about re-visiting aspects of the treaty framework and, particularly within the context of the Dark Net, making it more appropriate to the challenges of the twenty-first century.

Note on Structure and Methodology

This brief begins with a background to e-commerce drug transactions and the emergence of the Dark Net in order to situate readers unfamiliar with the history, language and technology of the hidden markets. It then examines the growth of these markets and the nature and impact of enforcement

responses before developing some concluding recommendations that look beyond the standard narrative of improvements to policing. The brief is based on primary and secondary source information and literatures. It incorporates interviews with Mike Power, author of *Drugs 2.0*, Dr Alexia Maddox of Deakin University and Curtin University, Australia and Dr Mark Houghton of Leeds University. Online interviews were conducted via a direct message facility with a sample of users of the Tor network. Discussion threads were posted on sites to allow anonymous online posting and interviews.

THE EMERGENCE OF ONLINE DRUG TRANSACTIONS

As outlined by Martin (2014),[5] illicit drugs have been bought and sold on the internet since it was first established. According to Markoff[6] (2005), cited in Martin, the first online ecommerce transaction was a 1971 marijuana exchange between students at Stanford University using the Arpanet accounts at the institution's Artificial Intelligence Laboratory and their counterparts at Massachusetts Institute of Technology. This underlines the 'dual use' challenge[7] that the advent of the internet posed for the IDCR, with unstoppable and positive advances in global communications creating an enabling environment for illicit drug supply and use.

The expansion of Personal Computer ownership and growth of internet access revolutionised how people communicated and retrieved information in relation to illicit drugs in the 1990s, a period of growth and expansion of the global drug trade following the fall of the Berlin Wall, the 'chemical revolution' of synthetic drug use[8] in Western Europe, North America and Australasia, the strengthening of cocaine and heroin supply from South America and South West Asia, and the emergence of Mexico as a geographic hub of drug distribution and manufacture. The internet provided a new, relatively anonymous and decentralised space

for the exchange of knowledge and experience of drug legislation, consumption effects and drug manufacture and cultivation, including through chat rooms and discussion forums that linked users across the world.

The 'alt' online newsgroup[9] pioneered this information sharing. Alt.drug and Alt.drugs.chemistry (created in 1994) hosted discussions including how to grow cannabis, manufacture synthetics (particularly MDMA and LSD), and where to purchase chemicals, equipment and paraphernalia. The online market for drugs transactions was initially conducted through Private Messaging (PM) facilitated by the newsgroup. The Hive, established in 1997 by Hobart Huson brought integrated market operations to the online trade. His Texas enterprise Science Alliance, which had an estimated annual $4 million turnover supplied the chemicals, equipment and instruction manuals for synthetic drug manufacture discussed on The Hive website.

Law enforcement was slow to respond to the emergence of internet based drug transactions, with the media initially playing an investigative role as with the exposure of Huson and the Hive operations by the 2001 NBC programme Dateline in its 'X Files' episode.[10] According to O'Neil 'At a time when the Internet was a fraction of its current size, police seemed either clueless or uninterested.'[11] This reflects the weakness of early warning systems, at both national and international levels, including within the UN system, to identify and respond to new drug market trends.[12] However, a key vulnerability of these websites was their ease of public access over the clear net (enabling law enforcement infiltration of user groups), and their use of traceable payment systems (Paypal, Pecunix, Western Union and cash in the post). These weaknesses contributed to the arrest of fifteen people connected to the Adam Flowers site,[13] which had processed approximately 5,256 online orders for controlled substances on the clear web valued at approximately $1,041,244 between January 2007 and October 2009.

TOR AND THE DARK NET

The early 2000s saw the emergence of cybercrime message forums such as ShadowCrew, counterfeitlibrary.com and the Russian language carderplanet.com operating on the clear web through a message board, with members communicating through a Virtual Private Network (VPN). Hosted in Hong Kong, ShadowCrew (2002) had approximately 2,500 members across an estimated seven countries that traded hacked, stolen and forged personal information such as credit card details, passports, birth certificates and driving licences, as well as hacking tools.[14]

Intercepted and closed following joint operations by US law enforcement and the UK Serious Organised Crime Agency (SOCA) in 2004, ShadowCrew:

Formed part of what the US Department of Justice described as "one of the largest illegal online centres for trafficking in stolen identity information and documents". The website acted as a criminal e-bazaar — in effect an online auction site for the underworld. By 2004 the international network had trafficked at least 1.7 million stolen credit card numbers and caused financial losses worth $4.3m (£2.1m)[15]

Outlining the challenge this type of transnational, remotely operated web based criminal network posed to traditional law enforcement, the head of e-crime at SOCA set out that ShadowCrew was distinct from the 'old-style "top down" organised crime groups:

Box 1: ShadowCrew Message Board

People have been used for specific skills, rather than the usual pyramid structure. With one person providing the documents, another would buy credit card details, another would create identities while another would provide the drop address […] "This is done without the people ever meeting."[16] (See Box 1).

Driving the growth of hidden markets was the release in 2002 of The Onion Router (Tor) 'a technology that bounces internet users' and websites' traffic through "relays" run by thousands of volunteers around the world, making it extremely hard for anyone to identify the source of the information or the location of the user'.[17] Developed through a partnership between the US Navy and the non-profit sector including Electronic Frontier Foundation, Knight Foundation and the Swedish International Development Agency (with the majority of funding provided by the US Department of Defence and State Department), Tor enables secure and confidential communication, 'designed to stop people – including government agencies and corporations – learning your location or tracking your browsing habits'.[18] The initial idea for an encrypted network was raised in 1996 at the First Information Hiding Workshop.

Tor provided anonymised web mail access through TorMail and hosted websites (such as the drug marketplaces) through hidden service capabilities accessed by downloading the Tor software on the open web.[19] As outlined on the Tor Project page 'Using Tor "rendezvous points," other Tor users can connect to these hidden services, each without knowing the other's network identity or physical location'[20] (Box 2).

Box 2: The Onion Router

The goal of Onion Routing is not to provide anonymous communication. Parties are free to (and usually should) identify themselves within a message. But the use of a public network should not automatically give away the identities and locations of the communicating parties. For example, imagine a researcher who uses the World Wide Web to collect data from a variety of sources. Although each piece of information that he retrieves is publicly known, it may be possible for an outside observer to determine his sensitive interests by studying the patterns in his requests. Onion Routing makes it very difficult to match his HTTP requests to his site.

David. M Goldschlag, Michael G. Reed & Paul F. Syverson, 'Hiding Routing Information, Workshop on Information Hiding, Cambridge, UK, 1996.

http://www.cs.jhu.edu/~fabian/courses/CS600.424/course_papers/goldschlag96hiding.pdf

Knowledge of the unique URL was previously required to locate hidden markets. However reflecting rapid advance of Dark Net technologies, the Grams search engine (discussed at the end of this paper) launched in 2014 enables searches across hidden market sites on the Tor.[21] Modelled on Google (Box 3), the advent of Grams brings a normalisation of activities on the hidden web, facilitating access to illicit markets.

Again with reference to the dual use dilemma facing the international drug control system and the wider UN framework of which it is a part, blocking Tor downloads to prevent illicit transactions is to the detriment of the software's important and intended role in anonymised communication. News

Box 3: Grams website

organisations, whistle-blowers and social activists – for example in Turkey, China and Iran use the Tor software to mobilise civil society and to publicise serious human rights abuses. According to O'Neill (2014), Tor had 40,000 users in Iran until Iranian authorities, like their Chinese counterparts, began to develop blocking tools to prevent Tor download:

Tor, an anonymity tool used by millions of people around the world for a wide variety of purposes, is a powerful and popular tool used in Iran by political activists and citizens looking to get around the country's strict speech and press laws. [22]

Since the US National Security Agency (NSA) leaks by Edward Snowden and WikiLeaks release of documents by Chelsea Manning, national governments and intelligence services have stepped up efforts to track communications and block Tor download. Nevertheless, Tor and hidden services continue to evolve with the development of new circumvention tools such as unlisted bridges and hidden paths to the Tor network. More recently Tor launched an .onion address for Facebook users[23] in response to ongoing privacy issues and to assist accessibility to social networks where these have been blocked. The end result is a technological 'arms race' that enables the refinement of Tor processes and continued expansion of increasingly robust and sophisticated Tor services, which as discussed below, have become the driver of adaptation and growth of online hidden drug markets.

DRUGS AND HIDDEN MARKETS

The first drug market to exist on the Tor network was The Drugstore, launched in 2009. According to Interviewee A, a former co-administrator of Drugstore:

The Drugstore was the first .onion drugs market that operated on the Tor network. Prior to that it was torture to get people to be secure! We tried to enforce PGP[24] and Tor on our forums prior to that but people just didn't listen and busts were rare back then I was involved in setting up further .onion sites […] During the onion forum era a huge amount of dealing was done via the PM system with E-mail only used by vendors who were not part of forums.

The second hidden service drug forum was A Figment of Your Imagination (AFOYI) followed by Binary Blue Stars (BBS) (See Box 4) 'a joking reference to the old rumour that people distributed LSD to kids on blue star stickers.' According to Interviewee A, this forum was 'pretty epic':

We had some huge acid dealers on it, we actually had our forum logo put on about a thousand sheets of acid that were distributed around the world so if you ever saw a sheet with two blue stars on it that was representing our community!

Box 4: Building the Early Drug Markets

BBS was the highly trusted forum, I think AFOYI was actually the forum we allocated for mid-level trusted people and then TLG (The Looking Glass) was for the least trusted people. Our goal was that we would get a lot of people on TLG and then if they proved to be legit we would promote them to AFOYI, and if they were still legit. And there for a long time they might make it to BBS if they had something to offer.

Interviewee A

Credibility was promoted through the allocation of vendors to a specific forum depending on the trust and the quality of their products.

From the trusted members on BBS, the idea of a totally public forum developed — the Open Vendor Database (OVDB), a move away from the existing market model of closed forums and privately organised groups. BBS, AFOYI and TLG were taken down, with OVDB launched around the same time as Silk Road 1.0. According to Mike Power, significant volumes of acid were moved across the OVDB with threads from vendors advertising the goods that they had to sell.

In terms of the financial transactions on the OVDB, interviewee A explains this began with Western Union, Money Gram, cash in mail, e-gold and then Liberty Reserve, a Costa Rica-based centralized digital currency service that enabled users to open accounts and transfer money with only a name, date of birth and email address.[25]

It was all on trust. You would have to open a Liberty Reserve account, put the money into the account and then encrypt the user name and password using PGP to that account and send it to the vendor, and send that via a private message system on the forum. The vendor would then take that money and cash it out.

As OVDB was launched, discussions emerged on its forums about Silk Road, which in addition to illegal drugs, sold clothing, art, books, music and computer and digital equipment (Boxes 5 & 6). When people accessed the site they found a professionally designed webpage where various categories of products were listed along with photographs.

Vendors had a short description and contact details that would normally contain their public key for PGP encryption (Box 7). The site had forums discussing and explaining the use of PGP, guiding new users in data encryption and decryption programming used for signing, encrypting, and decrypting texts, e-mails and other forms of electronic communication.

Box 5: Discussions about Silk Road

I came across this website called Silk Road. It's a Tor hidden service that claims to allow you to buy and sell anything online anonymously. I'm thinking of buying off it, but wanted to see if anyone here had heard of it and could recommend it. I found it through **silkroad420**.*wordpress*.*com, which, if you have a tor browser, directs you to the real site at* **http://tydgccykixpbu6uz**. **onion**. *Let me know what you think.*

Altoid's thread. January 27 2011, shroomery.org

Payment for goods and services on Silk Road were made in Bitcoin, an encrypted digital currency. In contrast to the vulnerabilities exposed by Paypal, Western Union and cash in post, this offered anonymity in financial transactions. The use of anonymous TorMail for private and anonymised communications between site users was another important security feature.

The screen shot on the adjacent page (Box 8) shows the rapid increase in the number of accounts opened on Silk Road, from 130 in February 2011 to 39,421 a year later.

Box 7: PGP Encryption

The PGP is based on two keys - one public and one private. Only the private key is known by the individual. The public key is published, an individual then copies the public key and information is encrypted using that key as a receiver of the encrypted information. This can then be de-crypted using the private key and password.

See the International PGP homepage for a detailed description http://www.pgpi. org/doc/pgpintro/

Box 6: Silk Road Site

Box 8: Silk Road Growth

```
series: [{
    name: 'Number of users by March 2012: 152,088',
    color: 'rgba(119, 152, 191, .5)',
    data: [
        [Date.UTC(2011, 0, 1), 5], /* 5 accounts created in January 2011, before the site went live */
        [Date.UTC(2011, 1, 1), 135], /* 130 accounts created in February 2011 */
        [Date.UTC(2011, 2, 1), 714], /* 579 accounts created in March 2011 */
        [Date.UTC(2011, 3, 1), 1381], /* 667 accounts created in April 2011 */
        [Date.UTC(2011, 4, 1), 2286], /* 905 accounts created in May 2011 */
        [Date.UTC(2011, 5, 1), 21991], /* 19705 accounts created in June 2011 */
        [Date.UTC(2011, 6, 1), 36904], /* 14913 accounts created in July 2011 */
        [Date.UTC(2011, 7, 1), 49477], /* 12573 accounts created in August 2011 */
        [Date.UTC(2011, 8, 1), 68328], /* 18851 accounts created in September 2011 */
        [Date.UTC(2011, 9, 1), 85888], /* 17560 accounts created in October 2011 */
        [Date.UTC(2011, 10, 1), 89676], /* 3788 accounts created in November 2011 */
        [Date.UTC(2011, 11, 1), 97486], /* 7810 accounts created in December 2011 */
        [Date.UTC(2012, 0, 1), 108568], /* 11082 accounts created in January 2012 */
        [Date.UTC(2012, 1, 1), 147989], /* 39421 accounts created in February 2012 */
        [Date.UTC(2012, 2, 1), 152088], /* 4099 accounts created in March 2012 */
    ]
}
```

Source: Runa Sandvik

Silk Road challenged the viability of OVDB, particularly as Silk Road received significant media publicity. A 2011 article 'The Underground Website Where You Can Buy Any Drug Imaginable' by Chen in *Gawker*, set out that:

Silk Road, a digital black market that sits just below most internet users' purview, does resemble something from a cyberpunk novel. Through a combination of anonymity technology and a sophisticated user-feedback system, Silk Road makes buying and selling illegal drugs as easy as buying used electronics— and seemingly as safe. It's Amazon—if Amazon sold mind-altering chemicals.[26]

Traffic to the site escalated as a result of media articles that introduced readers to the Dark Net. There was also positive feedback from Silk Road users, one buyer commenting that Silk Road 1.0 provided a smoother user experience compared to OVDB:

I like their trust system and the karma concept they have on the forums, but I haven't order from there as i feel the website is less user friendly than SR and so far I have had excellent experiences here so I don't feel i need to risk it[...] Having said that, OVDB is a great 2nd site. The more the merrier and it spreads the

LE bulls-eye around [...] which is good.

A few months after Silk Road had commenced trading, OVDB closed with the ex-administrator interviewee A reflecting that:

It just wasn't worth it for me anymore. DPR [Dread Pirate Robert, Silk Road founder] had a business model and a reason to keep running his site. SR went from a thousand members to tens of thousands to a hundred thousand from all the media attention and OVDB only had a few thousand at its peak. I decided it is better for us to just get behind Silk Road, and at the same time I figured actually that our entire model is not optimal. We should not have drug forums, we need a decentralized marketplace software that is NOT meant for use for illegal activity but is able to be used for ANY sort of market based site.

OVDB vendors, buyers and administrators moved over to Silk Road, which created an OVDB sub forum to attract tech-savvy users and facilitate the exchange of drugs in what was projected to become an increasingly competitive online marketplace.

CRYPTO CURRENCY AND BITCOIN

The key advantage of Silk Road 1.0 over competitors was the site's use of Bitcoin 'digital coins which are not issued by any government, bank, or organization, and rely on cryptographic protocols and a distributed network of users to mint, store, and transfer.'[27] Crypto currencies enable direct and anonymous transactions without oversight. These technologies enable online vendors and

buyers to communicate and exchange funds anonymously and with little risk of detection.

According to an interview with Dread Pirate Roberts, Silk Road emerged from an original idea to combine Bitcoin and Tor to create an anonymous market.[28] First devised by Satoshi Nakamoto in 2008, Bitcoin was launched in 2009 via a public post on an exclusive emailing list for cryptographers where Satoshi (2009) wrote 'Announcing the first release of Bitcoin, a new electronic cash system that uses a peer-to-peer network to prevent double-spending. It's completely decentralized with no server or central authority.'[29] For Satoshi the immediate problem Bitcoin faced was establishing its intrinsic value however as the popularity of Silk Road 1.0 grew, Bitcoin became the currency of choice within the drug marketplace forging a mutually beneficial relationship between the site and the crypto-currency, which reached a value of $9: 1 Bitcoin by mid-2011.

HIDDEN MARKETS AND HARM REDUCTION

The media brought Silk Road and hidden markets to the attention of politicians. In the US, Senator Chuck Schumer called on Federal Authorities to take action against Silk Road, which he described as 'a certifiable one stop shop for illegal drugs that represents the most brazen attempt to peddle drugs online that we have ever seen'.[30] Schumer expressed dismay that users rated the delivery performance of vendors and quality of the drugs that they bought on the site. While 'brazen', these activities appear to play an important and innovative role in the reduction of drug related harm.

Harm reduction approaches accept 'for better or worse, that licit and illicit drug use is part of our world and chooses to work to minimize its harmful effects rather than simply ignore or condemn them'.[31] Harm reduction principles acknowledge that some ways of using drugs are safer than others and 'affirms drugs users

themselves as the primary agents of reducing the harms of their drug use.'[32] As remote and anonymised transactions, hidden drug markets reduce the risks associated with illegal drug transactions with 'street dealers'.[33]

Harocopos and Hough[34] describe two retail market transactions; in closed markets, the customer is known to the vendor. In open markets, customer and vendors are not known to each other. The latter has traditionally been seen as the more dangerous owing to lack of trust between buyer and seller, the risk to both of physical exposure and arrest 'on the street', vulnerability to entrapment or violence, and the risk to the buyer of purchasing from strangers. Closed markets modify these risks but the buyer (and seller) can never guarantee drug type or purity, creating risk of illness and overdose. While hidden markets such as Silk Road reduce the barriers to purchasing, they also ameliorate the other dangers associated with open market transactions. According to one Silk Road user:

Before I found online drug markets I bought on urges and impulses from local wannabe gangsters, I had to call on the phone first to make sure things were cool then call to the house where I felt uncomfortable. There was sometimes the offer of more than I wanted on tick or try this, try that. I never did try any other drug from these wannabes but it was always there.

If the buyer is not satisfied with the product purchased from street dealers, or the buyer suffers complications from taking the drug due to other unknown substances in the product there is little chance of a refund, resolution or alerting other customers to defective, toxic or mis-sold drugs:

The street market is more risky for everyone. I would not want to sell from my house or my car to people face to face where I can be identified by several ways. Not only by police but by other rival dealers or gangs. The street market

doesn't have feedback or rating available for every buyer to read. You are more likely to be involved with people who might not be concerned in your welfare.' (SR Vendor)

According to Aldridge and Décary-Hétu the Dark Net drug markets are harm reducing as market influence and position are determined by technical know-how and not propensity for violence. Identifying Silk Road as a 'paradigm-shifting criminal innovation', they set out that violence in the traditional 'street' drug trade 'was commonly used to gain market share, protect turfs and resolve conflicts.' By contrast 'the virtual location and anonymity that the crypto market provides reduces or eliminates the need – or even the ability – to resort to violence.' As a result, while we must acknowledge that the potential of Dark Net drug markets to reduce traditional retail market violence is not the same across all countries and are currently most active in Europe, North America and Australasia — good customer service and writing skills 'may be more important than muscles and face-to-face connections.'[35]

A second harm reduction benefit of the hidden markets is the ratings systems pioneered by Silk Road. These are an important guide to the quality of products, reducing the likelihood of contamination, mixing and dilution with other products, overdose, and morbidity. As outlined by one Silk Road vendor, this is driven on the supply side by the prioritisation of market growth and related importance of customer care and feedback:

The advantage of Silk Road is your reputation is open to all. If you mess someone around its reflected in your feedback and ratings. The seller who wants good business on Silk Road has to try and make every customer happy. Customer service has never been this good on the street market. The downside as a buyer is having to trust the service with their money before the goods arrive and disclosing your personal details for delivery. The more

Box 9: Silk Road user comments

"MUCH safer, you know what your getting, you can see reviews of the product before you buy."

"The feedback system is revolutionary for a market like this. All my fears about quality are gone. I know what I'm getting and I know that it's good."

"Security of the transaction, less chance of violence, the rating and feedback system gives some confidence on the quality and substance;"

"Mostly I buy by vender reputation and buyer reports from the forums."

experience you have on Silk Road the more confident you get.' (SR vendor)

Chat rooms and discussion forums enable information and experience sharing on drug safety, optimal dosing and polydrug use that reduce the risk of serious harm or illness. They create a community of individuals in a non-judgemental environment where people feel safe to discuss drug related issues due to the anonymity provided by Tor (Box 9). For Bartlett 'Users and sellers alike can have the freedom to be open and express themselves in ways that are impossible in real life.'[36] Silk Road users highlight the harm minimising benefits of the site:

The community here is awesome. I mean look in the forums, there is a "Drug Safety" forum. The whole philosophy behind the place is that if you want to put heroin in your body, go ahead. But hey, if you want to get off that nasty drug, we're here to help you too. It's not like real life where street dealers might coerce you into keeping your addiction or whatever.

I read the forums [...] I sometimes take a chance, and I have never been ripped off or

sent fake drugs. That is pretty incredible, since online pharmacies usually you will be scammed 9 times out of 10, and even the ones who are given good reviews are usually sending pills that have been repressed with filler or illegal substances like heroin. I feel like people are less judgemental and pretentious here than on other websites.

Some users reported the site as having a regulating and moderating effect on their drug use:[37]

*I now control my consumption by ordering days or weeks (international) in advance and have found I smoke less but better quality
The Silk Road is a paradise for responsible drug dealers. I mean it's not the type of site where you can show up at your dealer's house banging on their door because you need your fix this instant. You have to be patient and you have to be smart to get there and use it.*

LAW ENFORCEMENT

In the 2014 *World Drug Report*, the rise of hidden, Dark Net drug markets was belatedly acknowledged. The *Report* set out that the variety of drugs available on the Dark Net appeared to be 'diverse and growing' and this posed 'unique challenges for law enforcement.'[38] As outlined by Interpol in the September 2014 Internet Organised Crime Assessment (iOCTA), the relationship between customer and vendor in the hidden markets is purely transactional. 'Criminals in cyberspace do not need to be close to the crime scene, they might never even travel to the target country', their activities can be conducted transnationally and 'with minimum effort and risk by hiding their identity', the Assessment notes. By contrast, in the off-line world 'criminals normally need to be physically present at the crime scene and can typically only commit one offence at a time.'[39]
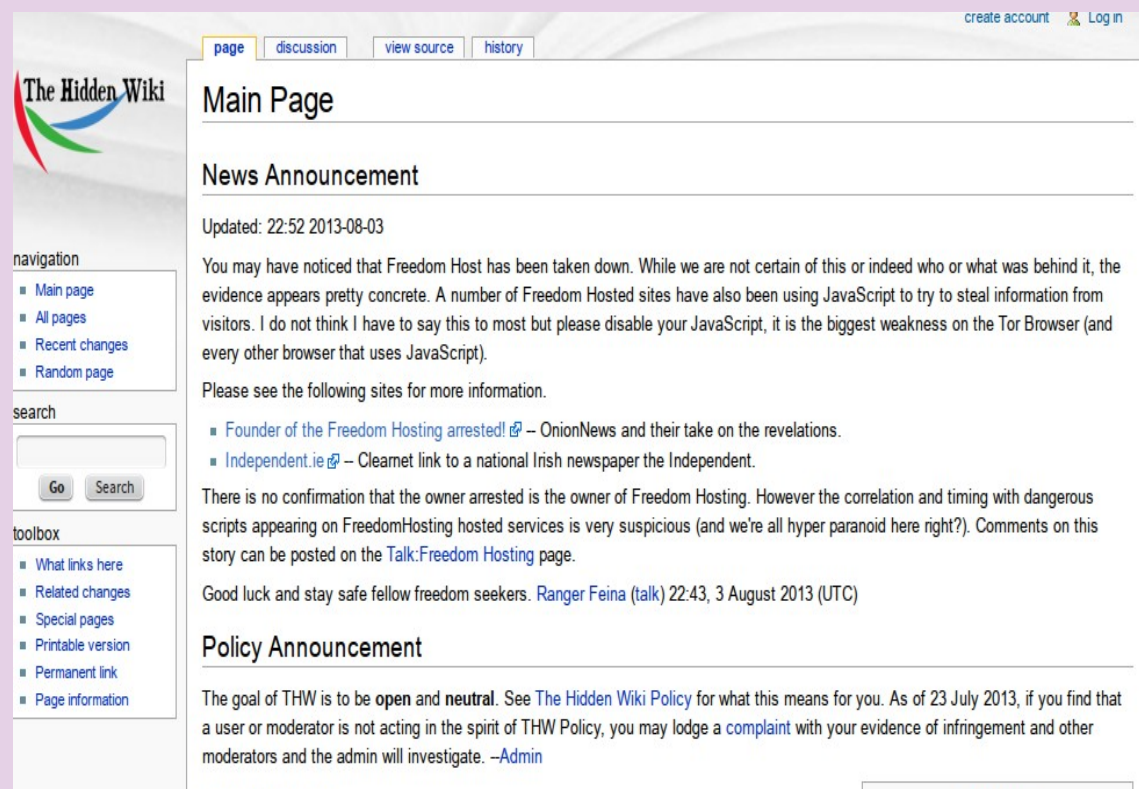
Law enforcement responses to the Dark Net have configured around traditional strategies of surveillance, interdiction and prosecution, although from a low base of technical capacity, with limited transnational integration and within the constraints imposed by national legislative frameworks. In a pattern that is familiar across the range of drug supply interdiction activities (crop eradication, targeting of so-called cartels, interception and seizure along trafficking and distribution networks), the effect of enforcement activities on the Dark Net has been to fragment and diversify drug markets, while catalysing innovation in security and counter surveillance, as discussed below.

In August 2013 an announcement was posted on Hidden Wiki (Box 10) that Freedom Hosting, a service inside the Tor network providing privacy tools that included TorMail, had been taken down by the US FBI and that its owner resident in Ireland had been arrested.[40] This followed an investigation into child sexual exploitation.

Servers of Freedom Hosting for TorMail, which included the entire e-mail database were seized, sending shockwaves through the hidden web. The FBI obtained a vast trove of e-mail, highlighting the importance of robust security protocol in hidden market transactions. As one Silk Road forum member set out:

I actually consider this thing a good thing because finally it will make people much more concerned about their security. I don't really think many people have something to really worry about (and I hope I'm right) but it's anyway a good "wake up" for people that this is not a joke. I see people here that used very obsolete versions of Tor, people that didn't encrypt their sensible info and trusted a third-party site, people that didn't know the difference between having Java Script enabled or not, people (and even worse vendors) that just used Tor bundle and that's it thinking they are secure just for this.

Box 10: Law Enforcement Responses

It removed the veneer of invincibility […] a lot of people using Silk Road got complacent (including me, sending unencrypted addresses and such), and therefore stopped using DNMs[41] for a while afterward. If the biggest can go down, any can and this hopefully has led to increased security for other markets ow.

Arrests following the seizure were widely reported in the media, ensuring continued high profile coverage of Silk Road and hidden markets.[42] Two months after Freedom Hosting's closure, the FBI arrested San Francisco based Ross William Ulbricht as the alleged Silk Road operator Dread Pirate Roberts and seized assets of the site (Box 11), primarily 29,000 Bitcoins valued at approximately $5 million.[43] The FBI described Silk Road as 'the most sophisticated and extensive criminal marketplace on the Internet' with a turnover of $1.2 billion and generation of $80 million in commissions for its administrators.

With Silk Road down, vendors and buyers immediately shared contact email addresses and public keys. The effect of closing the site was not to prevent the sale or purchase of drugs; rather it drove communications further underground, while increasing user attention and knowledge of security issues. underground, while increasing user attention and knowledge of security issues.

Box 11: FBI Notification of Silk Road Take Down

A second consequence of Silk Road's interdiction was a rise in registration on other Dark Net sites such as Black Market Reloaded and Sheep Marketplace, which provided a mechanism for verifying trusted Silk Road vendors in order to encourage their customers to follow. Just as the interdiction and break-up of Colombia's Medellin 'cartel' and assassination of its leader Pablo Escobar had no impact on levels of cocaine supplied from Colombia, so closing Silk Road and arresting Dread Pirate Roberts had no long term or catastrophic impact on the Silk Road project or hidden markets more broadly; quite the reverse. It stimulated new competition, innovation in business models and the launch of Silk Road 2.0 as communicated by Libertas one of the moderators on Silk Road in November 2013:

I would like to announce our new home http://silkroad5v7dywlc.onion

As I have always stated, even with Silk Road itself, you should act at all times as though any site or marketplace you visit has been compromised from the very beginning. That is the only way to ensure that you do not become lax with your security. Do not fall into a false sense of security at any time on any site. Do not get comfortable. When you get comfortable you get confident, when you get confident you get cocky, and when you get cocky you get caught. With the necessary security warnings out of the way, I look forward to seeing you all over on the new site. Let LE [Law Enforcement] waste their time and resources whilst we make a statement to the world that we will not allow jackbooted government thugs trample our freedom. We are born free, yet moments later we are shackled by the rule of law. It is time, once again, to break free of those shackles.

Demonstrating a high level of flux and dynamism in the illicit marketplace following the closure of Silk Road 1.0 in 2013 and the termination of its near monopoly on hidden market drug transactions, a plethora of new sites emerged.

Operations in the free market of the Dark Net environment were highly competitive, with weak 'firms' that were incapable of ensuring the market premium of robust security quickly closed down — as was the case with Sheep Marketplace following the theft of £3.3 million Bitcoins and also Atlantis in September 2013, which posted on its clear web Facebook page:[44]

We have some terrible news. Regrettably it has come time for Atlantis to close its doors. Due to security reasons outside of our control we have no choice but to cease operation of the Atlantis Market marketplace. Believe us when we say we wouldn't be doing this if it weren't 100% necessary. Due to the urgency we are allowing all users to withdrawal (sic) all their coins for one week before the site, and forum, are shut down permanently. Please remove all of your coins; these will not be recoverable after one week from now. Anything remaining in your accounts will be donated to a drug related charity of our choosing. We wish to thank all of you for making Atlantis a great and memorable place to trade on. We wish you all the best in your future endeavours.

By contrast, the use of third generation authentication features and sophisticated marketing and advertising campaigns by sites and vendors — such as discount offers on bulk drug purchases and free samples, enabled new market entrants to thrive and consolidate. These include Evolution, which by end of October 2014 had 17,512 listings and a 28 per cent market share of total listings, Agora with 17,200 listings and a 27.5 per cent market share and Silk Road 2.0 with 15,837 listings and a 25.3 per cent market share. Comprising 81 per cent of total listings, these three market places contributed to 41 per cent of online Dark Net market places between May and October 2014. According to Mike Power, arrests and the closure of Silk Road version:

Has inadvertently been the most brilliant advertising for hidden web drug markets. The FBI have acted as the most creative marketing

and advertising agency that the hidden web drugs sector could have possibly have hoped for. According to Alexia Maddox 'when the volatility of the drug market grabbed onto the vendors they knew and went underground', in turn complicating the already onerous challenge posed by the hidden markets to law enforcement. The market places have continued to evolve and expand in 2014 as new sites such as Agora, Evolution and Pandora came on line. At the time of writing, Dark Net Stats cite a figure of forty-five current live sites.

Following a joint operation by the 16-member states of Europol, the FBI, US Immigration and Customs Enforcement (ICE) and Homeland Security,[45] twenty seven hidden market sites were closed in November 2014, including Silk Road 2.0 (Box 12). However, Box 13 demonstrates that the transaction volume of the closed sites represents less than a third of the drug markets and that the much publicised impact of this enforcement operation was overstated.

In response to the seizure of Silk Road 1.0 and now 2.0 new decentralised open source markets are emerging such as Dark Market and Open Bazaar, which means the code is publicly available. According to its developer[46] OpenBazaar (Box 14) is a new way to trade online with Bitcoin users:

By running a program on your computer, you can connect directly to other users in the OpenBazaar network and trade with them. This network isn't controlled by a company; it's a decentralized network that isn't run by any organization at all. This means there are no mandatory fees to pay, and that your trade is censorship-resistant. OpenBazaar uses Bitcoin,

Box 12: Hidden Market Closure Notification 2014

Box 13: 2014 Seizures Source: Digital Citizens Alliance

reliable information about these parts of the Dark Net was to read forums and subreddits. I wanted to make it easier for users to use the Dark Net. Grams has made Dark Net information more accessible to normal users and because of its publicity has brought a lot of new users to the Dark Net. I think it has also
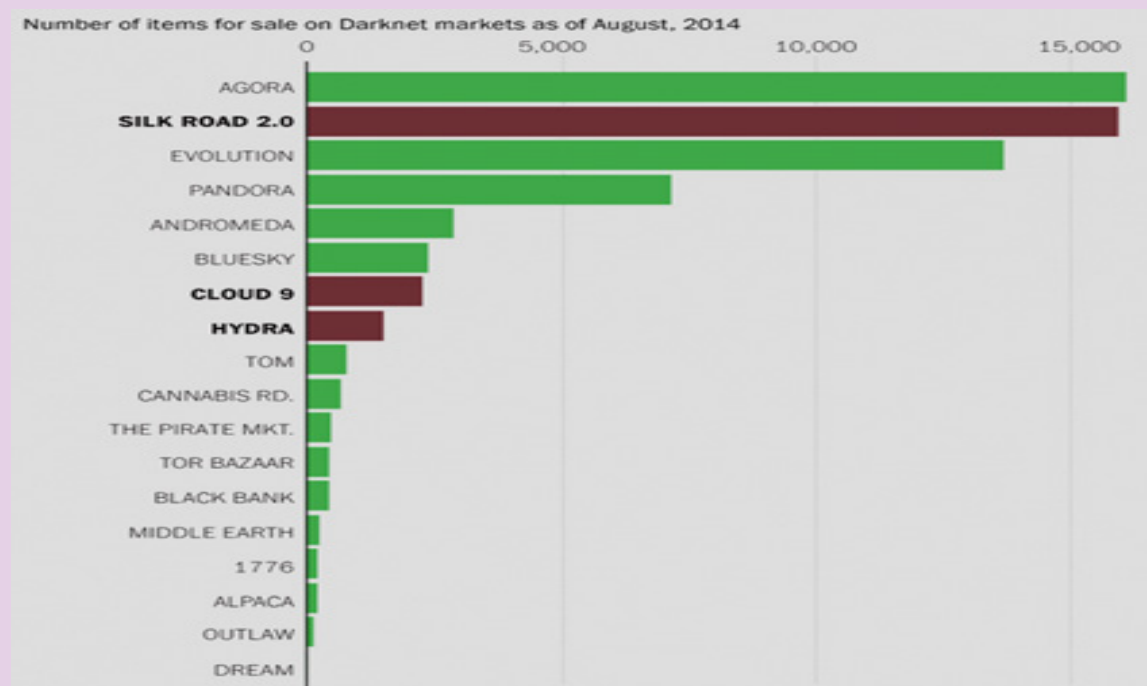
a digital currency that is also cheap to use, decentralized, and censorship-resistant.

Maddox outlines that 'People are constantly looking at different parameters on how they can sustain the market places. I do believe there are new market place concepts being worked up as we speak that will transform how business is done. The markets have adapted and will continue to adjust to market driven needs for the foreseeable future. Digital relationships will form and dissolve depending on the emerging risks and opportunities.'

Interdiction of Silk Road, continued demand for illicit drugs, advances in online security technology and crypto currencies, and the scale of profits to be generated from drug sales will ensure that the hidden markets will continue to adjust to consumer demands. Moreover hidden web activities will become more accessible through innovations like the Grams search engine and normalised through the trend of advertising activity an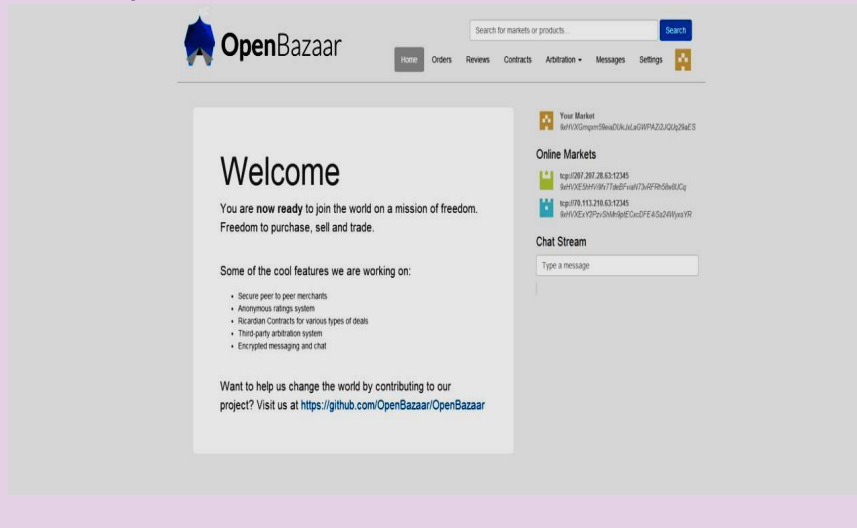d links on the clear web. The developer of Grams, which receives around 10,000 searches and 6,000 unique visitors a day, set out that:

I created grams because 90% of the Dark Net was behind black market sites which required a login to view. This made it unsearchable by normal search engines. The only real way to get

raised the bar for Dark Net sites. Before grams a lot of the sites we not very well designed or easy to use. I think Grams set a new standard for what a Dark Net site could be. I like to think of the Dark Net as the internet reborn [...] The Dark Net can be much more. It can be a safe haven for people who want change but are afraid to speak because of governing laws or repercussions to themselves and/or their families. I hope Grams can help it grow into what it needs to be.[47]

This adaptation has transformed how people can search the hidden web and access the vendors by name without having to log onto various sites. It has received favourable reviews from reddit users.

I still use Grams to compare prices and vendors without having to log into different sites. I love it!

Grams impresses the hell out of me for all the little things he works on to makes markets more usable. The engine is truly impressive and he really does work toward giving people what they want. I believe a lot of vendors have at least a few customers who discovered them via GS.

It allows you to find where a certain vendor has set up shop if you can't find them on your own, and it gives you access to all the customer

feedback they have all in one place. It really makes things a lot easier when trying to find legit vendors for something and for sniffing out the bad ones as well.

When Silk Road 1.0 was closed, commentators predicted a crash in **B**itcoin's value. However, just as the Dark Nets bounced back and strengthened as a result of law enforcement efforts, Bitcoin rebounded rising to $305 within weeks. Ugo Egbunike, director of business development at Index Universe stated 'I thought Silk Road is going to do some damage to the price but with BTC China buying this up — they seem to have picked up the slack.'[48] Underlining recognition of Bitcoin as a viable and legitimate currency and its normalisation outside of Dark Net transactions, the German government will impose capital gains tax on Bitcoin trading,[49] and the Chief Executive of Visa stated that the company was open to facilitating the use of Bitcoin.[50] The Superintendent of the New York Department of Financial Services revealed a draft proposal in 2014 of regulations governing virtual currencies like Bitcoin. If passed, they will be the first regulations on virtual currencies anywhere in North America to carry the full weight of the law.[51]

CONCLUSIONS

Hidden drug markets are projected to experience exponential growth influenced by multiple dynamics that include expanding internet access; the emergence of a new tech-savvy generation; the development and ease of security tools; the evolution of crypto currencies, and – most significantly, sustained international demand for illicit drugs. The value of the Dark Net drug markets and incentives to engage in supply are a factor of the illegality of drugs, while criminalisation of the trade will continue to drive efforts to develop alternative, 'risk free' (or reduced risk) transaction chains. The internet is

generating rapid change in the illicit drug trade, providing an accessible and efficient mechanism for global marketing and sales.[52] These will become more professionalised and consumer oriented, underpinned by an expanding interface with the clear web and social media – as most recently exemplified by Facebook's decision to enable user connections directly to the Tor.

Serious and complex challenges exist in dis-embedding the (increasingly *less*) hidden drug markets, which evolve from the bottom up rather from the top down, respond efficiently to market conditions and which lack a physical infrastructure, enabling vendors to quickly relocate their business in response to enforcement pressures.[53] As demonstrated by the 'successful' closure of Silk Road 1.0 and more recently Silk Road 2.0, surveillance and interdiction efforts, including through the tracking of crypto currencies and efforts to block Tor downloads generates new and relentless innovation in technologies and encryption. Even in a hypothetical scenario of complete and sustainable hidden drug market interdiction and closure, the impact will be simply to return drug trading to more harmful street markets.

Traditional law enforcement strategies and policing techniques are inadequate to confront the full range of Dark Net and hidden services available, and that pose challenges in terms of locating servers and uncovering encrypted, anonymised identities dispersed internationally among individuals rather than hierarchically organised criminal gangs. As outlined by Europol in the 2014 iOCTA report 'it appears that EU law enforcement, Europol included, has not fully conceptualised how to integrate this cyber dimension into all relevant aspects of police work, let alone devise a strategy and implementation plan to make this happen.' The transnationalised nature of the hidden markets render national level policing strategies and evidence gathering largely ineffectual, while simultaneously posing

complex questions in relation to prosecution. As outlined in an interview with Houghton:

Have the police got the resources to put into policing the online markets? Who is responsible? Is it the responsibility of the country where the server exists? do they know where the server is? It's the classic problem of dealing with transnational crime, where exactly does the offense take place, is it at the point of transaction or at the point of possession?

To date, enforcement has relied on the use of informants, undercover surveillance, tracking, hacking, exploitation or creation of security breaches (for example through the use of malware) and high publicity 'take downs' intended to alarm and intimidate users, vendors, and host service providers, including through the message that no interactions can ever be anonymous and always risk arrest and prosecution.

The problem with these approaches, as with much anti-drug rhetoric, is that the audience can become quickly inured to the articulated threat and risk. Moreover in seeking to contain and disrupt hidden markets through traditional policing techniques and by bending established legislation to new challenges, law enforcement risks becoming increasingly reckless in its violations of civil liberties as seen with the use of the US Patriot Act of 2001, which was intended as a counter-terrorism measure:

When it was signed into law six weeks after the [9/11] attacks, the act made it easier to wiretap American citizens suspected of cooperating with terrorism, to snoop through business records without notification, and to execute search warrants without immediately informing their targets (a so-called sneak-and-peek). Privileges once reserved for overseas intelligence work were extended to domestic criminal investigations. There was less judicial oversight and very little transparency. The bill's symbolism mattered also, signalling that the moral deference previously given to the Special Forces would be broadened

until it encompassed much of the apparatus of the American state. Local prosecutors, military policemen, CIA lawyers—these were indispensable patriots too.[54]

A decade after its introduction, the Patriot Act had been used in only fifteen terrorism cases but 1,618 drug cases. [55]

One strategy used to push back on-line drug sales relates to the prosecution of postal services and courier firms, as seen in the fining of UPS and indictment of FedEx Corp for money laundering in relation to the delivery of medications without prescription from on-line, clear web pharmacies, which, like the Dark Net hidden markets, have experienced exponential growth. This strategy, extending to surveillance and interception of private mail, encourages innovation in delivery methods[56] and faces legal challenge from postal companies. According to the trade journal *Post and Parcel* in relation to the FedEx case, the shipping company was of the view that the lawsuit tests the concept of privacy within the business of shipping, placing on the carrier legal responsibility for the contents of packages being transported. As such, FedEx noted,

We will plead not guilty [...] We will continue to defend against this attack on the integrity of FedEx. We continue to ask for a list of all internet pharmacies engaging in illegal activity so we can turn off shipping for those companies immediately. We have asked for a list, and they have sent us indictments." [...] FedEx was ready to work with law enforcement to tackle the issue, but insisted "the responsibility to monitor, regulate or police the activities of doctors and pharmacists lies with licensing, regulatory and law enforcement authorities, not shipping companies.[57]

International and national level law enforcement acknowledge the capacity, logistical, technical and financial constraints they face in dealing with the hidden markets and the Dark Net

more broadly. Recommendations to address these limitations typically focus on enhancing the skills, resource and legal base of counter narcotics actors and agencies, including through improvements to cross border cooperation in intelligence sharing and interdiction operations.

This recourse to conservative and traditional mainstream solutions severely underestimates the scale of the capacity building required. They are largely unsophisticated in their proposals for the directing of (increasingly scarce) resources and, as discussed in this brief and as evidenced in other areas of the drug trade, strict enforcement efforts often only fragments and expands the hidden markets. As such a rigid law enforcement approach risks increasing harm rather than promoting the 'well-being of mankind', a core objective of the UN treaty system as set out in the 1961 Single Convention on Narcotic Drugs and the framework within which national legal systems operate. Additionally the focus on hidden drug markets detracts resources and capacity from 'industrial level' criminality in relation to child sexual exploitation, as recently outlined by the UK Prime Minister.[58]

An alternative approach to the challenge of the popular, expanding and dynamic hidden drug markets is one based on harm reduction principles, 'market management'[59] oriented evidence based approaches and a pragmatic response to dramatically changing internet technologies:

1   There must be investment in ethical, well-funded research and analysis of the interactions of hidden drug markets, and vendor / user dynamics. This should address the extent to which review systems that reward sellers of 'quality' products reduce the risk associated with drug consumption; how hidden market operations impact violence associated with street dealing, and how far chat rooms and discussion forums — as open and anonymous spaces for discussion — provide an entry point for drug support

services,[60] particularly for users isolated from mainstream services due to problematic use or concerns over identification.

2   The research of Aldridge and Décary-Hétu[61] among others demonstrates that the most frequently transacted drugs are moderate and organic substances such as cannabis (and niche drugs such as magic mushrooms and khat), not drugs associated with problematic use and chaotic lifestyles such as heroin or methamphetamine. More and better information about the types of drugs transacted on the rapidly increasing number of sites is required in order to prevent interventions that disrupt 'soft' supplies and drive vendors and buyers into deeper and 'harder' markets, and in order to better identify and support the needs of chaotic users who typically do not purchase from the Dark Net. Responses to the hidden markets must learn the lesson of previous enforcement errors, and avoid unsophisticated catch-all strategies.

3   The diversification of drug sites has enabled users to make ethical choices about the sites where they will buy drugs. More research is required to substantiate emerging evidence that the online drug community reject marketplaces that also for example sell / exchange images of child sexual exploitation or weaponry. Law enforcement activities against what are in many respects self-regulating and 'ethical' communities is counterproductive while conversely a virtual *modus vivendi* offers the opportunity for the exchange of information relating to high end criminal activities that many Dark Net drug enthusiasts deplore. Knowledge relating to internal hidden market communities, regulations and codes of conduct will support intelligence gathering as this relates to the most serious cyber-crimes, is in line with Europol's need, acknowledged in the 2014 Internet Organised Crime Assessment to build 'new alliances.'

4   Law enforcement should focus skills and resources on high level organised and predatory cyber-crime including child and female sexual exploitation, financial crime, weapons trafficking, cross border cyber-attacks and cyber terrorism. As outlined in a *Computers at Risk* report by the US National Research Council from 1991 'Tomorrow's terrorist may be able to do more with a keyboard than with a bomb.'[62] There consequently needs to be hierarchy of security risk when assessing cyber enforcement priorities, with non-violent and consensual drug transactions on the Dark Net relegated to the minor role that these activities play in the generation of illicit cyber revenues and social threat.

5   The growth of hidden markets and the Dark Net more broadly evokes sensationalist statements and publicity from politicians, the media and law enforcement. Public opinion and policy responses must not be framed by panic and fear of emerging technologies. A primacy must be placed on information, explanation and evidence, particularly to bridge generational divides over technology literacy and use.

6   It was opposition to the 'war on drugs' approach and to law enforcement dominated strategies applied to achieve a 'drug free world' — as, among other places, prominently laid out in the slogan for the 1998 UNGASS on the World Drug Problem — that brought civil libertarians and drug 'enthusiasts' together on the internet to develop the first online drug information exchanges, archives , databases and ultimately drug markets. It is the prohibition for recreational purposes of certain substances that makes their supply so lucrative and this underpins the growth surge enjoyed by Dark Net drug sites as internet and social media use has and will continue to expand rapidly. The 2016 UNGASS offers a timely opportunity to begin to defuse the projected rate of Dark Net drug market growth. In the short to medium term, the international community should consider creating policy space within which to manage better Dark Net drug markets rather than solely seeking to eliminate them and undermine the harm reduction benefits that they appear to offer. In relation to longer term goals, the rapid expansion and dynamic nature of these non-traditional markets also adds to the already growing pressure for a re-evaluation of the current prohibition-oriented international framework and catalyses the need for serious discussion of a formal shift towards regulated markets for some currently illicit substances; a once heretical call that is now gaining traction.[63]

It is acknowledged that hidden drug markets can introduce people to drugs that might otherwise not be accessible, that drugs bought on the internet can cause harm and that harm reduction benefits may not be equally distributed across states, regions and markets. Nevertheless, these real dangers and concerns are outweighed by the harms caused by current or any future strategies based on efforts to simply disrupt and dislocate Dark Net supply.

ENDNOTES

1   J. Buxton, (2006), The Political Economy of Narcotics: Production, Consumption and Global Markets, London: Zed Books

2   Cyberterrorism 'refers to unlawful attacks and threats of attack against computers, networks and the information stored therein that are carried out to intimidate or coerce a country's government or citizens in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear'. D. Denning (2000) Cyberterrorism: The Logic Bomb versus the Truck Bomb', *Global Dialogue*. 2:4. p. 29.

3   UNODC (2014) *World Drug Report*. UNODC: Vienna. p. 18.

4   For example see A. Stevens (2013) 'Applying Harm Reduction Principles to the Policing of Retail Drug Markets', *Modernising Drug Law Enforcement*. Report 3. International Drug Policy Consortium.

5   J. Martin (2014) *Drugs on the Dark Net: How Cryptomarkets are Transforming the Global Trade in Illicit Drugs*. London: Palgrave Macmillan.

6   J. Markoff (2006) *What the Dormouse Said: How the Sixties Counterculture Shaped the Personal Computer Industry*. London: Penguin Books.

7   Other dual use problems for the UN drug control system for example include opioids, which are classified by the WHO as essential medicines, but which are strictly controlled to prevent abuse. Due to the tight strictures imposed by the treaty fraemwork on access and distribution of opioids, an estimated 90 per cent of the global population are denied pain alleviating drugs in the treatment and palliative care of chronic and terminal illness.

8   Amphetamine Type Substances (ATS) such as MDMA, amphetamine and methamphetamine.

9   The 'alt' online newsgroup was founded by John Gilmore and computer scientist Brian Read.

10 Sections of the programme can be viewed here http://www.youtube.com/watch?v=WOafo1y77R8

11   P. Howell O'Neill (2013) 'How the Internet Powered a DIY Drugs Revolution'. *The Daily Dot*. August 28. http://www.dailydot.com/crime/hive-silk-road-online-drug-culture-history/

12 This lack of early warning capacity can be extrapolated beyond internet drug sales to include the rise of synthetic drug markets in the 2000s and Novel Psychoactive Substances in the 2010s.

13 See Jablon (2012) 'Farmer's Market' International Online Drug Ring Busted, 15 Arrested. *Huffington Post* April 16. http://www.huffingtonpost.com/2012/04/16/international-online-drug-market-busted-arrests_n_1429544.html . On the DEA Operation Adam Bomb that led to the arrests see *Operation Adam Bomb*: Arrest of Creators, Operators of Online Secret Narcotics Marketplace. http://www.justice.gov/dea/pubs/pressrel/pr041612a.html The indictments can be accessed at   http://

www.wired.com/images_blogs/threatlevel/2012/04/WILLEMSIndictment-FILED.045.pdf The Youtube video demonstrates the workings of the Adam Flowers site, https://www.youtube.com/watch?v=rIE_SMUBIx0

14 On the emergence and development of the cybercrime market see L. Ablon, M. Libicki and A. Golay (2014) *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar*. Rand Corporation. http://www.rand.org/pubs/research_reports/RR610.html

15 L. Rodgers (2007) Smashing the criminals' e-bazaar. *BBC News*. December 20. http://news.bbc.co.uk/1/hi/uk/7084592.stm

16 Rodgers, BBC News. *Ibid*.

17 S. Dredge (2013) 'What is Tor? A Beginner's Guide to the Privacy Tool', *Guardian*. November 5. http://www.theguardian.com/technology/2013/nov/05/tor-beginners-guide-nsa-browser

18 Dredge ibid.

19 www.torproject.org

20 For the technical details of how the rendezvous protocol works see https://www.torproject.org/docs/hidden-services.html.en

21 See http://www.reddit.com/r/DarkNetMarkets/comments/22jg6b/darknet_markets_search_engine/

22 P. Howell O'Neill (2014) 'Iran blacklists Tor network, knocking 75 percent of users offline', *Daily Dot*. July 30. http://www.dailydot.com/politics/iran-censors-tor-75-percent/ See also XB Emerging Technology (2012) 'How China Blocks the Tor Anonymity Network', *MIT Technology Review*. April 4. http://www.technologyreview.com/view/427413/how-china-blocks-the-tor-anonymity-network/

23 https://facebookcorewwwi.onion/

24 Pretty Good Privacy (PGP) encryption. See the International PGP homepage for a detailed description of how this works http://www.pgpi.org/doc/pgpintro/

25 See BBC Technology News (2013) 'Liberty Reserve digital money service forced offline'. May 27. http://www.bbc.co.uk/news/technology-22680297

26 A. Chen (2011) 'The Underground Website Where You Can Buy Any Drug Imaginable', *Gawker*. January 6. http://gawker.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160

27 D. Ron and A. Shamir, no date, *Quantitative Analysis of the Full Bitcoin Transaction Graph*. https://eprint.iacr.org/2012/584.pdf

28 A. Greenberg (2013) 'An Interview With A Digital Drug Lord: The Silk Road's Dread Pirate Roberts (Q&A)', *Forbes Magazine*. August 14. http://www.forbes.com/sites/andygreenberg/2013/08/14/an-interview-with-a-digital-drug-lord-the-silk-roads-dread-pirate-roberts-qa/

29 See S. Nakamoto. (2009) Re: Bitcoin v0.1 released. http://www.mail-archive.com/cryptography@metzdowd.com/msg10152.html and also http://sourceforge.net/p/bitcoin/mailman/bitcoin-list/?viewmonth=200901

30 J. Ball. (2013) 'Silk Road: the online drug marketplace that officials seem powerless to stop', *Guardian*. March 22. http://www.theguardian.com/world/2013/mar/22/silk-road-online-drug-marketplace

31 Harm Reduction Coalition: Principles of Harm Reduction http://harmreduction.org/about-us/principles-of-harm-reduction/

32 Harm Reduction Coalition: Principles of Harm Reduction http://harmreduction.org/about-us/principles-of-harm-reduction/

33 M.C. Van Hout and T. Bingham. (2013) 'Responsible vendors, intelligent consumers: Silk Road, the online revolution in drug trading', *International Journal of Drug Policy*. 25:2. pp. 183–189

34 A. Harocopos and M. Hough (2011) 'Drug Dealing in Open-Air Markets', *Problem-Oriented Guides for Police Problem-Specific Guides Series*. Guide No. 31

35 J. Aldridge and D. Décary-Hétu (2014) 'Not an 'Ebay for Drugs': The Cryptomarket 'Silk Road' as a Paradigm Shifting Criminal Innovation'. Available at SSRN: http://ssrn.com/abstract=2436643 or http://dx.doi.org/10.2139/ssrn.2436643

36 J. Bartlett (2014) *The Dark Net: Inside the Digital Underworld*. London: Heinemann.

37 See M.C. Van Hout and T. Bingham. (2013) 'Silk Road', the virtual drug marketplace: a single case study of user experiences', *International Journal of Drug Policy*. 24: 5. Pp 385-391.

38 World Drug Report 2014. Ibid. p. 18

39 Europol's 2014 Internet Organised Crime Assessment (iOCTA) can be found at https://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta

40 J. Hawes (2013) 'Freedom Hosting arrest and takedown linked to Tor privacy compromise', *Naked Security*. August 5. http://nakedsecurity.sophos.com/2013/08/05/freedom-hosting-arrest-and-takedown-linked-to-tor-privacy-compromise/

41 Dark Net Markets. Statistical information can be obtained at Dark Net Stats http://dnstats.net/

42 K. Hill (2013) 'How A Delaware Doctor Was Linked To Silk Road Drug Sales', *Forbes Magazine*. November 26. http://www.forbes.com/sites/kashmirhill/2013/11/26/how-a-delaware-doctor-was-linked-to-silk-road-drug-sales/

43 BBC Technology News (2014) 'Seized Silk Road bitcoin hoard sold in US'. June 30. http://www.bbc.co.uk/news/technology-28085722

44 https://www.facebook.com/AtlantisMarket/posts/421945931244529

45 https://www.europol.europa.eu/content/global-action-against-dark-markets-tor-network

46 https://openbazaar.org/

47 Interview with T. Bingham

48 O. Kharif (2013) 'Bitcoin Climbs to Record on Wider Acceptance, China Trade', *Bloomberg News*. June 11. http://www.bloomberg.com/news/2013-11-06/bitcoin-climbs-to-record-on-wider-acceptance-china-trade.html

49 R. Dillet (2013) 'Germany Recognizes Bitcoin As "Private Money", Sales Tax Coming Soon,. *Techcrunch* August 19. http://techcrunch.com/2013/08/19/germany-recognizes-bitcoin-as-private-money-sales-tax-coming-soon/

50 B. Head (2014) 'Visa aims to make future payments friction-free'. http://www.afr.com/p/technology/visa_aims_to_make_future_payments_8IucuVjza7XuuItJVsqdhL

51 See P. Rizzo (2014) 'Ben Lawsky: New York Can't Risk Getting Bitcoin Regulation Wrong', *Coindesk*. August 21. http://www.coindesk.com/ben-lawsky-bitcoin-regulation/ Also B. Lawsky. (2014) ' Regulations of the Superintendent of Financial Services Part 200: Virtual Currencies', available at: http://www.dfs.ny.gov/about/press2014/pr1407171-vc.pdf

52 See T. Seddon (2014) 'Drug Policy and Global Regulatory Capitalism: The Case of New Psychoactive Substances (NPS)', *International Journal of Drug Policy*. 25: 5. Pp.1019–1024.

53 D. Bright and J. Delaney (2013) 'Evolution of a Drug Trafficking Network: Mapping Changes in Network Structure and Function across Time', *Global Crime*. 14: 3. P. 238-260.

54 B. Wallace-Wells (2011) 'Patriot Act: Kitchen Sink Approach to National Security', *New York Magazine*. August 27. http://nymag.com/news/9-11/10th-anniversary/patriot-act/

55 Ibid

56 Including potential future use of private drones

57 *Post and Parcel* (2014) 'FedEx faces more charges over shipping of illegal prescription drugs'. August 18. http://postandparcel.info/62280/news/companies/fedex-faces-more-charges-over-shipping-of-illegal-prescription-drugs/

58 N. Morris (2014) 'New police unit will track down paedophiles on dark net', *Independent*. December 11. http://www.independent.co.uk/news/uk/crime/new-police-unit-will-track-down-paedophiles-on-the-dark-net-9916533.html

59 See, International Drug Policy Consortium, International Institute for Strategic Studies and Chatham house, Modernising Drug Law Enforcement Seminar Report, pp. 8-9 http://idpc.net/policy-advocacy/special-projects/modernising-drug-law-enforcement.

60 See for example T. Duffin. (2014) 'Opinion: A new drug trade is hiding in the underbelly of the internet', Available at : http://www.thejournal.ie/readme/dark-net-drugs-silk-road-1452620-May2014/

61 J. Aldridge and D. Décary-Hétu, ibid.

62 D. Denning (2000) Cyberterrorism: The Logic Bomb versus the Truck Bomb', *Global Dialogue*. 2:4. ibid.

63 See for example, Global Commission on Drug Policy, *Taking Control: Pathways to Drug Policies that Work*, September 2014 http://www.gcdpsummary2014.com/#foreword-from-the-chair

supported by

OPEN SOCIETY FOUNDATIONS

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
Global Drug
Policy Observatory

reporting monitoring analysis

@gdpo_swan