palgrave pivot

DRUGS ON THE DARK NET

How Cryptomarkets Are Transforming the Global Trade in Illicit Drugs

James Martin

Drugs on the Dark Net

DOI: 10.1057/97811373990052.0001

Other Palgrave Pivot titles

Shin Yamashiro: **American Sea Literature: Seascapes, Beach Narratives, and Underwater Explorations**

Sudershan Goel, Barbara A. Sims, and Ravi Sodhi: **Domestic Violence Laws in the United States and India: A Systematic Comparison of Backgrounds and Implications**

Gregory Sandstrom: **Human Extension: An Alternative to Evolutionism, Creationism and Intelligent Design**

Kirsten Harley and Gary Wickham: **Australian Sociology: Fragility, Survival, Rivalry**

Eugene Halton: **From the Axial Age to the Moral Revolution: John Stuart-Glennie, Karl Jaspers, and a New Understanding of the Idea**

Joseph Kupfer: **Meta-Narrative in the Movies: Tell Me a Story**

Sami Pihlström: **Taking Evil Seriously**

Ben La Farge: **The Logic of Wish and Fear: New Perspectives on Genres of Western Fiction**

Samuel Taylor-Alexander: **On Face Transplantation: Life and Ethics in Experimental Biomedicine**

Graham Oppy: **Reinventing Philosophy of Religion: An Opinionated Introduction**

Ian I. Mitroff: **The Crisis-Prone Society: A Brief Guide to Managing the Beliefs That Drive Risk in Business**

Takis S. Pappas: **Populism and Crisis Politics in Greece**

G. Douglas Atkins: **T.S. Eliot and the Fulfillment of Christian Poetics**

Guri Tyldum and Lisa G. Johnston (editors): **Applying Respondent Driven Sampling to Migrant Populations: Lessons from the Field**

Shoon Murray: **The Terror Authorization: The History and Politics of the 2001 AUMF**

Irene Zempi and Neil Chakraborti: **Islamophobia, Victimisation and the Veil**

Marian Duggan and Vicky Heap: **Administrating Victimization: The Politics of Anti-Social Behaviour and Hate Crime Policy**

Pamela J. Stewart and Andrew J. Strathern: **Working in the Field: Anthropological Experiences across the World**

Audrey Foster Gwendolyn: **Hoarders, Doomsday Preppers, and the Culture of Apocalypse**

Sue Ellen Henry: **Children's Bodies in Schools: Corporeal Performances of Social Class**

Max J. Skidmore: **Maligned Presidents: The Late 19th Century**

Lynée Lewis Gaillet and Letizia Guglielmo: **Scholarly Publication in a Changing Academic Landscape**

Owen Anderson: **Reason and Faith at Early Princeton: Piety and the Knowledge of God**

DOI: 10.1057/9781137399052.0001

palgrave pivot

Drugs on the Dark Net: How Cryptomarkets Are Transforming the Global Trade in Illicit Drugs

James Martin
Senior Lecturer, Macquarie University, Australia

palgrave
macmillan

DOI: 10.1057/9781137399052.0001

First published 2014 by
PALGRAVE MACMILLAN

Palgrave Macmillan in the UK is an imprint of Macmillan Publishers Limited, registered in England, company number 785998, of Houndmills, Basingstoke, Hampshire RG21 6XS.

Palgrave Macmillan in the US is a division of St Martin's Press LLC, 175 Fifth Avenue, New York, NY 10010.

Palgrave Macmillan is the global academic imprint of the above companies and has companies and representatives throughout the world.

Palgrave® and Macmillan® are registered trademarks in the United States, the United Kingdom, Europe and other countries.

ISBN: 978–1–137–39906–9 EPUB
ISBN: 978–1–137–39905–2 PDF
ISBN: 978–1–137–39904–5 Hardback

A catalogue record for this book is available from the British Library.

A catalog record for this book is available from the Library of Congress.

www.palgrave.com

DOI: 10.1057/9781137399052

To Emilia, and Mani

DOI: 10.1057/9781137399052.0001

Contents

DOI: 10.1057/9781137399052.0001

Acknowledgements

This book would not have been possible without the generous assistance of colleagues, friends and family. At Palgrave Macmillan, thanks to Julia Willan and Harriet Barker for their encouragement and patience. From Macquarie University, I wish to thank Julian Droogan, Zara Bending, Yvonne Breyer and Peter Anderson. In the broader academy, thanks are also due to Alastair Fraser, Dean Wilson, Clifford Shearing and Jennifer Wood (for the nodes – again), and particularly to Jude McCulloch for her expert guidance and advice. Closer to home, thanks too to Christopher Blain, David Woodfield and Rob Loader for excellent insights and discussion. Final, extra special thanks to Carol Aeschliman for countless hours of reading and feedback, and to Emilia Martin for her constant support and encouragement.

DOI: 10.1057/97811373990520002


palgrave pivot
www.palgrave.com/pivot

Introduction

Abstract: *This section introduces the reader to key terms and themes used throughout the book, including cryptomarkets, cryptocurrencies and the TOR network. The scope and aims of the book are outlined and research questions identified.*

Martin, James. *Drugs On the Dark Net: How Cryptomarkets Are Transforming the Global Trade in Illicit Drugs.* Basingstoke: Palgrave Macmillan, 2014. DOI: 10.1057/9781137399052.0003.

This book is about online drug dealing. More specifically, drug dealing which is carried out on an encrypted part of the internet called the TOR network, otherwise known as the *dark net*. Illicit trading on the dark net has only recently come to the attention of the general public and academia. This newfound awareness is due partly to the spectacular rise and fall of the infamous online drugs bazaar, *Silk Road*. Despite being a relatively new area of scholarly inquiry, illicit drugs have been bought and sold on the internet practically since its inception. According to Markoff (2005), the very first online transaction of any kind took place in the early 1970s and involved a marijuana exchange between students at MIT and Stanford University. From this inauspicious beginning, online drug dealing has developed dramatically. Fuelled by the global proliferation of powerful communications and encryption technologies, illicit drugs are now readily accessible whenever anyone connects online.

The two technologies upon which dark net drug traders are dependent are TOR (*The Onion Router*) encryption and cryptocurrencies. TOR is a free "circuit based low-latency communication service" that was developed in partnership with the non-profit sector and the US military (Dingledine, Mathewson et al. 2004: 1). Launched in 2002, TOR facilitates anonymous communications and web browsing, enabling users to interact online without revealing their identity or physical location. Cryptocurrencies are a more recent innovation. The most widely used cryptocurrency is Bitcoin which began operating in 2008 (Nakamoto 2008). Cryptocurrencies facilitate direct and anonymous transactions between parties without the involvement or oversight of external financial institutions. The combined use of these technologies means that online drug traders are able to communicate and exchange funds anonymously and with relatively little risk of detection (Barratt, Ferris et al. 2013, Martin 2013, Aldridge and Décary-Hétu 2014).

Drugs are available on the internet through a variety of means. Ubiquitous spam emails spruik prescription medications (typically related to issues regarding male 'performance') which are sold by online pharmacies of dubious reliability (Orizio, Merla et al. 2011). On a much smaller scale, encrypted storefronts have recently begun populating the TOR network, offering a limited range of illicit goods from hidden, centralised locations (DeepDotWeb 2014). This book focuses on a particular kind of online illicit site known as a dark net marketplace or *cryptomarket*. A cryptomarket is defined as "an online forum where goods and services are exchanged between parties who use digital encryption to conceal

DOI: 10.1057/9781137399052.0003

their identities" Martin (2013: 356). They share a range of further characteristics which help distinguish them from other dark net enterprises, as well as from illicit sites operating on the legitimate, 'surface' web. These include:

- Reliance on the TOR network
- Third-part hosting and administration
- Use of traditional postal systems to deliver goods
- Decentralised exchange networks
- Use of encrypted electronic currencies or 'cryptocurrencies' (e.g. Bitcoin). (Martin 2013)

In describing the operation of cryptomarkets, commentators often draw parallels with legitimate online marketplaces, characterising them as a sort of 'eBay of illicit drugs' (Barratt 2012, Heintz 2012, Ormsby 2012). Despite the cliché, this analogy is broadly accurate. As is the case with legitimate online trading forums, cryptomarkets do not actually sell anything. Rather, they host the infrastructure necessary for buyers and sellers to conduct transactions amongst themselves. The role of a cryptomarket is therefore as a facilitator and broker rather than a direct participant in the illicit exchange. The decentralisation, distance and anonymity inherent to cryptomarket-facilitated exchanges are key aspects of their flexibility and durability. Decentralised exchange networks are able to expand rapidly, connecting as many users as the site infrastructure can handle. The idiosyncrasies of encrypted online exchange also make cryptomarkets extraordinarily difficult targets for law enforcement agencies which have more organisational experience and expertise in prosecuting in-person forms of illicit exchange (Christin 2013, Martin 2013).

The decision to write this book was prompted by the growing sense of alarm amongst some sections of the commentariat regarding the potential dangers associated with the online drugs trade. In many ways cryptomarkets constitute a 'perfect storm' of potential crime hysteria and moral panic. They combine two emotive and often little understood issues – illicit drugs and the dark net (as well as the internet more generally) – evoking fear and suspicion amongst the general public. Many of the concerns regarding cryptomarkets are well founded: they directly facilitate drug-related crime, particularly retailing and manufacturing; they are accessible to anyone with an internet-enabled computer, a bank account and a minimal level of technical proficiency, including children;

DOI: 10.1057/9781137399052.0003

and have also been implicated in the deaths of drug users around the world, especially young people (Deutsch 2013, Whitehead 2013, Jivanda 2014). There can be little doubt, therefore, that cryptomarkets are associated with a range of serious harms.

That sourcing illicit drugs online may result in harm is not, in itself, a particularly revealing or useful observation. The various dangers associated with the consumption of illicit drugs (e.g. overdose, addiction) are well known – though commonly overstated (Nutt 2012) – and it is little surprise that their use, regardless of how they are sourced, may sometimes result in serious injury or even death. A more productive line of inquiry is whether cryptomarkets present a more or less harmful alternative to the conventional illicit drugs trade. This is a complex question, and there is not yet sufficient research available to answer it conclusively. However, the particular dynamics associated with this uniquely 21st century form of drug distribution suggest a range of benefits over interpersonal dealing and distribution, particularly in reducing systemic drug-related violence and organised crime (Martin 2013, Aldridge and Décary-Hétu 2014).

This book is an exploratory work intended to stimulate further discussion and research about the online drugs trade. The aim is to provide a conceptual, empirical and non-technical contribution to the study of cryptomarkets. It focuses on four research questions, each with its own chapter:

1. What are cryptomarkets and how can existing scholarship contribute to understanding of these sites?
2. How do cryptomarkets operate from a commercial perspective?
3. How do conventional drug distribution networks differ from those facilitated online?
4. What is the relationship between cryptomarkets and the state? What are the challenges associated with policing the online drugs trade?

To address these questions, this book presents qualitative research gathered on the dark net. The main sources of data are discussion threads available on publicly accessible cryptomarket forums, as well as on vendor profile pages where illicit goods are advertised. While illicit drugs appear to be the primary commodity traded on cryptomarkets, many of these sites also deal in a broader range of illicit goods and services, including firearms, computer hacking services and stolen credit card information (Christin 2013). Analysis of these non-drug goods and services is outside the scope of this study.

DOI: 10.1057/9781137399052.0003

1
Conceptualising Cryptomarkets

Abstract: *The first chapter is intended to ground the concept of the cryptomarket in broader scholarly knowledge and aims to present these illicit sites as complex and multifaceted entities. Online drug dealing is discussed in relation to various definitions of cybercrime. Cryptomarkets are also analysed as sites of informal nodal governance, and various nodal resources, mentalities, technologies and institutions are identified. Finally, users of cryptomarkets are analysed as interdependent and resilient online communities with complex notions of collective and political identity.*

Martin, James. *Drugs On the Dark Net: How Cryptomarkets Are Transforming the Global Trade in Illicit Drugs*. Basingstoke: Palgrave Macmillan, 2014. DOI: 10.1057/9781137399052.0004.

Cryptomarkets are complex computer-based phenomena. In cyberspace they represent virtual meeting places for a motley assortment of deviants, drug users, entrepreneurs and political activists who come together online to share information and to trade. Whilst logged on to a cryptomarket, the physical location and identity of users are masked by free yet highly sophisticated encryption technology. This enables anonymous communications and commerce, the nature of which is often subversive or illegal, particularly with regard to the use, sale and distribution of illicit drugs (Barratt, Lenton et al. 2013, Christin 2013, Hout and Bingham 2013, Martin 2013, Van Hout and Bingham 2013). The diverse range of illicit products which are traded via cryptomarkets, together with their clandestine nature, contributes to a popular misunderstanding that these virtual spaces are entirely lawless where 'anything goes'. This perception is fuelled by sensationalist media reporting, with one news article recently likening cryptomarkets to the infamous *Star Wars* cantina at Mos Eisley Spaceport (Lumby 2013), a 'wretched hive of scum and villainy' where, for the right price, one can buy virtually anything.

Whilst colourful and evocative, the *Star Wars* analogy is also misleading. As is demonstrated later in the chapter, the majority of cryptomarkets strictly prohibit the sale of the most overtly and unambiguously harmful goods and services (such as child pornography and contract killing, to mention two examples which are frequently, and often erroneously, cited by the news media) (Falconer 2012, Palmer 2012, Lumby 2013). That commentators draw on inaccurate and misleading language and imagery of science fiction in describing cryptomarkets is revealing, as it points to a deficit in both popular and academic terminology that is capable of adequately explaining these new forms of association developing on the internet. This is not a problem particular to criminology or any other academic discipline. The recent mass proliferation of advanced communication technologies poses an ongoing challenge to scholars across the breadth of the academy to develop new concepts and theories which are relevant to an increasingly interconnected age. The rapid pace of technological change is also problematic as it contrasts significantly with the traditionally more ponderous cycles of academic observation, analysis, peer-review and debate. This mismatch often leaves scholarly discourse lagging significantly behind online events and places an additional emphasis on the timely development of conceptual tools with which one may interrogate and analyse novel online phenomena.

DOI: 10.1057/9781137399052.0004

This chapter further develops the concept of the cryptomarket by drawing on other, more established scholarly concepts and theories. A central aim is to explore these illicit sites as complex and multifaceted entities that fulfil a variety of functions. As a starting point, the criminal dimensions of cryptomarkets are discussed with reference to the emergent and loosely defined field of cybercrime. The focus of the analysis is then broadened to incorporate non-criminal perspectives, identifying cryptomarkets as spontaneously forming and self-regulating sites of nodal governance. Finally, cryptomarkets are analysed as idiosyncratic online communities which share a range of values and attitudes with regard to illicit drug use and exchange.

Cryptomarkets and cybercrime

To date, much of the public and scholarly discourse regarding cryptomarkets refers to cybercrime (Hodson 2013, Ablon, Libicki et al. 2014, Trautman 2014). This ubiquitous and overly inclusive term refers to practically any offence committed with the help of a computer, ranging from simple harassment carried out via email, to global 'botnet' attacks which are capable of paralysing critical national infrastructure (Provos, Rajab et al. 2009). To provide much-needed clarity and depth to the concept of cybercrime, scholars have created a range of cyber-taxonomies. These include simple binary classifications, such as the dichotomy between 'computer-assisted' and 'computer-oriented' or 'computer-focused' crimes. This well-known system differentiates traditional sorts of offences that are committed with computer assistance (e.g. fraud, blackmail, breaking and entering) from entirely new, virtual offences such as hacking and malware creation (Jewkes, Yar et al. 2010). Similar to this are taxonomies which categorise computer-related crimes according to their perceived association with various types of conventional offences. For example, the unauthorised access of private, virtual space may be conceived as 'cyber-trespassing', while injurious online offences such as bullying and harassment represent forms of 'cyber-violence' (Wall 2001, Holt 2013). More recently developed cybercrime taxonomies include those that cluster offences according to whether offenders use computers as either targets or tools (or both) (Brenner 2010), or alternatively refer to different stages in the chronological development of computer-related

DOI: 10.1057/9781137399052.0004

offences and the increasing risks/costs posed to private enterprises (Sjouwerman 2011).

Among the more sophisticated of cyber-taxonomies are the '3 generations' of cybercrime identified by Wall (2007). Wall's (2007) system distinguishes between computer-related offences according to the degrees to which they utilise and exploit global computer networks. Determining the generation to which a computer-related offence is associated is achieved by performing a hypothetical 'transformation test'. This involves hypothesising how the offence would be affected if computer networks were no longer available. According to Wall (2007), first-generation cybercrimes are those which are able to continue essentially unchanged in the absence of computer networks. These are traditional sorts of offences that use computers for communications or other practical purposes, but may also employ substitute means to perform these tasks if computer networks are unavailable. An example of a first-generation cybercrime is a burglar who uses a computer to disable the alarm on a bank vault. In this case, the exploitation of a computer network may be useful, or perhaps even critical to the commission of the offence. However, in the hypothetical absence of computer networks, burglars will almost certainly continue to steal from banks through the use of alternate means. The computer network is therefore simply another tool used in the commission of what is otherwise a conventional offence. While perhaps more technologically sophisticated than other instances of burglary, it does not qualitatively differ from similar offences that do not rely upon the use of computer networks.

By contrast, second-generation cybercrimes are those which exploit some of the vast new criminal opportunities afforded by global computer networks (Wall 2007). These too may resemble conventional types of offences, but are also significantly transformed by the availability of networked systems. The dissemination of child pornography is perhaps the most troubling example of a second-generation cybercrime. This offence pre-dates the mass proliferation of networked computer systems so it is clear, both historically and hypothetically, that it is able to persist in their absence. However, the scope and magnitude of the offence is significantly transformed by computer networks and associated communications technologies. These allow offenders to meet online and to communicate with one another with ease and relative anonymity, as well as facilitating the instantaneous transfer of much greater volumes of illegal data than would otherwise be possible through conventional,

DOI: 10.1057/97811373990520004

interpersonal networks of offenders. If one transforms the offence by removing computer networks, then the dissemination of child pornography would undoubtedly continue, but only in much smaller volumes and at a significantly reduced rate.

Third generation cybercrimes also exploit global computer networks, but they do so through the use of automated software (Wall 2007). Computer automation dramatically increases the scale of third generation cybercrimes relative to other cyber-offences because, once created by a skilled programmer, automated programs are able to self-replicate without further active participation on the part of offenders. The dissemination of malware which infects and 'enslaves' computers via spam email is one of the most common and costly examples of a third generation cybercrime (Wall 2007). Upon opening malware concealed in a spam email, cyber-victims unwittingly forfeit some degree of control over their computer, which is then incorporated into a global network of similarly compromised 'botnets'. This network expands automatically by accessing personal information that is stored on comprised hard drives or email accounts and generating subsequent spam attacks. These in turn compromise more computers and perpetuate the cycle of infection and expansion. The power of this 'viral' method of transmission depends upon both computer automation and networked systems and, importantly, if one hypothesises their removal, then the offence would effectively cease to exist.

Of the three generations of cybercrime identified by Wall (2007), only the first two are currently relevant to cryptomarkets. However, identifying whether offences committed via cryptomarkets constitute either first or second-generation cybercrimes is more complicated than it may initially appear. At first glance, the primary offence facilitated by cryptomarkets (i.e. the sale of illicit drugs) appears to correspond to the criteria associated with first-generation cybercrimes. This is because the vast bulk of the global illicit drugs trade is carried out not through the use of computer networks, but rather through interpersonal networks of drug manufacturers/cultivators, wholesales, traffickers and local distributors (see Chapter 3 for more detailed discussion of conventional drug distribution networks). These conventional drug distribution groups may use computer networks to communicate and help coordinate their activities. However, if one performs the Wall (2007) transformation test and hypothesises their removal, then it is clear that both the sale and distribution of illicit drugs would persist by other means. For this

DOI: 10.1057/9781137399052.0004

reason, Wall (2007) specifically identifies drug dealers who use computer networks as committing first-generation cybercrimes.

Complicating this perspective, however, is the fact that the sale of illicit drugs carried out *via cryptomarkets* is dependent upon global computer networks. Cryptomarkets transform conventional drug sales by facilitating the creation of global networks of offenders. These networks comprise both vendors and purchasers of illicit drugs who, once online, are able to conduct a range of illicit activities not only on an unprecedented scale, but also with a degree of freedom that significantly exceeds what is possible through conventional, interpersonal criminal networks. Particularly, cryptomarket users may readily compare and purchase tens of thousands of different illicit products from vendors located all over the world (Christin 2013). They may communicate freely, instantaneously and anonymously with one another, as well as access and contribute feedback about the huge variety of products that are listed for sale. Information provided in this manner is then automatically processed by cryptomarkets in order to rank the multitude of registered illicit vendors according to perceived reliability and customer satisfaction (see Chapter 2 for more detailed discussion of cryptomarket operations and consumer feedback systems).

The vast scale of cryptomarket-facilitated computer networks, combined with the speed, flexibility and reciprocal nature of online communications, significantly transforms the sale of illicit drugs when compared to similar offences committed via conventional illicit markets. Critically, if one hypothesises the removal of computer networks, then cryptomarkets, and the highly sophisticated and extraordinarily user-friendly drug exchange services that they provide effectively cease to exist. This suggests that cryptomarkets facilitate a form of illicit drug sales that is qualitatively different from the conventional, offline variety. Unlike conventional, offline drug sales, cryptomarket-facilitated drug offences are dependent upon, and significantly transformed by, global computer networks and therefore represent second-generation, rather than first-generation, cybercrimes.

Nodal governance

While cryptomarkets may be analysed as sites for the commission of cybercrime, by focusing exclusively on their criminal dimensions scholars risk ignoring or underemphasising other important aspects about the roles and functions in cyberspace. An alternative to

DOI: 10.1057/97811373990520004

a criminal-centric perspective is to consider cryptomarkets as sites of informal nodal governance on the internet. The concept of nodal governance was originally developed by Shearing and Wood (2003) as a way of mapping the plurality of public and private authority structures operating within neo-liberal states. According to Shearing and Wood (2003), the broad range of institutions involved in contemporary governance may each be conceived as interconnected nodes operating within a broader network of governing structures. Governing nodes are located within four sectors: state, corporate or commercial, non-government, as well as final, 'informal' category comprised of groups which are not located within any other sector. In many countries, nodes across all of these sectors perform a variety of roles previously conceived as within the remit of the state, including the provision of essential services, such as healthcare, education, security and policing (Loader and Walker 2004, Wood and Dupont 2006, Hein, Burris et al. 2010). Under a nodal conception of governance, state institutions are not afforded conceptual priority over nodes located in other sectors. Rather, governance is perceived as fluid and decentralised, with both public and private nodes expanding, contracting, and reconfiguring their relationships with one another and with the general public as circumstances demand.

Of particular relevance to the study of cryptomarkets are criminal groups which emerge as informal governing nodes. This happens most readily in regions where state, commercial and non-government institutions are either underdeveloped or completely absent (Martin 2013). Spaces that suffer from this form of formal 'governance deficit' are typically encountered in failed or failing states, or in areas excluded or alienated from formal governing institutions and mainstream economic activity, for example, in 'first world' urban slums and ghettos. In these areas, informal groups in the form of gangs, mafias and insurgents emerge as substitute, pseudo-governments that may provide vital sources of employment, security and even rudimentary forms of social welfare (Weinstein 2008, Brands 2010, Martin 2013). Other sites also suffering from a deficit in formal governance and therefore routinely attracting informal governing nodes are black markets. Prohibited trades, whether in illicit drugs, banned firearms or exotic and endangered wildlife, are, by definition, unable to be directly regulated by either state or (law-abiding) commercial institutions. In their absence, informal governing nodes, particularly organised crime groups, carry out a range of regulatory functions more usually associated with formal governing institutions, including the enforcement of informal rules

DOI: 10.1057/9781137399052.0004

and business contracts, dispute resolution and the provision of security (Volkov 2002, Martin 2013).

Cryptomarkets as informal governing nodes

Nodal governance, whether formal or informal, is ideally adaptable to cyberspace. The idea of governance as a complex network of interconnected nodes corresponds seamlessly to the physical network of interconnected hard drives and internet servers that together comprise the World Wide Web. Even the various designations of websites as either state (.gov), commercial (.com) or non-governmental organisation (.org) readily demarcate to which sector a governing node belongs (fourth sector, informal governing nodes lack a similarly clear online designation. However, given that the TOR network was established as a means of evading state oversight and control (Bradbury 2014), it seems reasonable to posit that sites operating on this encrypted part of the internet fit within this general, informal fourth sector). The following sections explain how cryptomarkets meet the more detailed requirements necessary to be designated informal governing nodes.

According to Burris, Drahos et al. (2005), in order to constitute a governing node an organisation must exhibit the following four characteristics: mentalities, technologies, resources and institutions. In this context, *mentalities* refers to a "way of thinking about matters that the node has emerged to govern" (Burris, Drahos et al. 2005: 37). Nodal mentalities include organisational cultures, philosophies, political ideologies or even more loosely defined collective attitudes and predispositions. These are expressed through a variety of mechanisms, including both formal (e.g. organisational charters, mission statements, constitutions) and informal (e.g. discourses, oral histories, songs). *Technologies*, by contrast, help translate nodal mentalities into purposeful action and refer to the various methods employed by a governing node to control and influence events. Examples of nodal technologies include standard operating procedures, business plans, military strategies and project management systems. Nodal technologies are implemented through the use of *resources*, which include assets that are either physical (e.g. money, computer hardware) or non-physical (e.g. specialist expertise). Finally, nodal *institutions* represent the formal and informal organisational hierarchies, frameworks and divisions of labour operating within a governing node. They are persistent organisational structures that enable the "directed mobilization of resources, mentalities and technologies over time" (Burris, Drahos et al. 2005: 38).

DOI: 10.1057/97811373990520004

Cryptomarket mentalities

Nodal mentalities are often expressed formally through cryptomarkets in the form of organisational charters. Perhaps the most notable example of this kind is the charter formerly hosted on *Silk Road 1.0* (see Figure 1.1). This remarkable document was written and posted by the administrator of *Silk Road 1.0*, *Dread Pirate Roberts*, and articulates an idealistic, even utopian set of principles intended to guide interactions between users and inform the governance of site operations. Expressed throughout the *Silk Road 1.0* charter are commitments to universal human rights and libertarian values.

Silk Road Charter

Silk Road is a global enterprise whose purpose is to empower people to live as free individuals. We provide systems and platforms that allow our customers to defend their basic human rights and pursue their own ends, provided those ends do not infringe on the rights of others.

***Our mission** is to have voluntary interaction between individuals be the foundation of human civilization.*

We conduct ourselves and our enterprise from the following fundamental values that are at the heart of who we are:

Self-ownership

Individuals own their bodies, thoughts and will. Anything they create with their property or obtain without coercion is also theirs.

Responsibility

People are responsible for their actions. If one infringes on another's rights, the victim has the right to defend themselves.

Equality

Property rights apply to all individuals equally, without exception.

Integrity

Honoring one's word as one's self. Word, thought, and action are aligned.

Virtue

Striving to improve one's self and the lives of others in all actions. To create value.

We promise to be true to our purpose, to accomplish our mission, to operate consistent with our values, and to run our enterprise in service of our customers.

This is who we are.

This is what you can count on.

FIGURE 1.1 *Silk Road 1.0 Charter [accessed 10/2/2012].*

DOI: 10.1057/9781137399052.0004

Not all cryptomarkets formally communicate their values in such lofty terms. However, a commitment to libertarianism is consistently encountered across many sites. Nearly all of the those surveyed as part of this research hosted 'Politics & Ethics' discussion forums where users debate various political issues, particularly drug prohibition and policing, and the value of cryptomarket trading as a less violent alternative to the conventional illicit drugs trade. Unsurprisingly, there is often strong support for libertarian political philosophies which rationalise illicit drug trading as a response to perceived unnecessary state intrusion into the lives of drug vendors and consumers (Barratt, Lenton et al. 2013).

> I do consider myself a libertarian. Unless the community here realizes that the only way we survive is by totally supporting one and other....buyers and sellers doing what ever is necessary to help each other out and to stand together against a government who seems hell bent on being our nanny.
>
> *User post – Pandora forum [accessed 15/5/2014]*

> I just want to... help unite us all under one flag and to continue spreading the libertarian ideology that means so much to me.
>
> *Moderator post – Silk Road 1.0 [accessed 10/12/2012]*

Ethical and responsible conduct on the part of online drug traders is a similarly popular topic for discussion on cryptomarket forums. One of the most widely read and commented upon discussion threads in the 'Philosophy, Economics and Justice' forum hosted on *Silk Road 1.0* was titled '[An] Ethical Code As A Freedom Fighter In The Drugs War'. The initiator of this thread proposed ten principles that outlined ethical conduct for cryptomarket users, including providing accurate information to consumers about drug purity, appropriate dosages and harm reduction measures, as well as a commitment to the safe disposal of toxic wastes that may be produced as a by-product of illicit drug manufacture. In response to largely supportive comments made by other users, the initial poster made the following rationalisation for writing the ethical code:

> I wrote that list as I was reading a bunch of government propaganda tonight about how all drug dealers are evil and prey on kids and it really got me angry so I thought it was important to clarify my own ethical code in the way I conduct myself. Just because we take or sell mind-altering substances does not make us any less ethical than any other person from another walk of life.

DOI: 10.1057/97811373990520004

There is, of course, no practical way of establishing either the veracity of this statement or the commitment to these principles on the part of this user and their apparent supporters. Also, even if these righteous sentiments are genuinely held, they are not necessarily reflective of a broader consensus amongst other cryptomarket users. Indeed, many users express scepticism about the value and relevance of political ideology and righteous sentiments, and instead advocate 'politics free' values such as honesty, professionalism and accountability (Van Hout and Bingham 2013).

> Ideals mean nothing way down here at the bottom of the web. Honesty is key. This is the only ideal.
>
> *User post – Pandora forum [accessed 17/5/2014]*

> SR [Silk Road] has become to [sic][1] much of an ideology, something that people but faith in rather then a business that should be scrutinized and analyzed at every turn.
>
> *User post – Silk Road 2.0 forum [accessed 18/5/2014]*

It is clear that there are a diverse range of views across cryptomarkets about the political and ethical dimensions of online drug trading. It is, therefore, not being argued that organisational charters or ethical discussions necessarily indicate that those involved with cryptomarket-related drug dealing are generally motivated by more noble or higher-minded ideals than their contemporaries in the conventional, offline illicit drugs trade. However, what these statements do clearly reflect are 'ways of thinking' about online drug sales and distribution that transcend immediate, operational practicalities such as product delivery, profit maximisation or security. As such, they embody nodal mentalities, irrespective of whether they are articulated formally by a site administrator, as in the example of *Silk Road 1.0* charter, or informally and spontaneously by users on cryptomarket forums.

Cryptomarket technologies

While users of cryptomarkets express varying levels of enthusiasm for the political ideologies and debates that are relevant to online drug trading, all online drug vendors and consumers depend upon nodal technologies whenever using an illicit site. Nodal technologies explicate the means by

DOI: 10.1057/97811373990520004

which drugs may be bought, sold and delivered via a cryptomarket. They are most clearly expressed as user guides which outline various website rules and the processes involved with making an online transaction. For example:

Basic rules

1. *New vendors with less than 20 transactions can not ask for early finalize (even for new customer – you still have option for cancel order, if you are not willing to accept risk).*
2. *Items which are* not allowed*: child porn (and other sick stuff), services, that can harm people (murder, etc.)*
3. *Vendor MUST public PGP PUBLIC KEY, so customers are able to send encrypted messages (like address).*
4. *VENDOR must pay security fee to be able to sell on PANDORA (we don't want kid scammers here).*

Excerpt from *Pandora* vendor guide; emphasis in original [accessed 9/5/2014]

Clearly articulated rules and procedural guidelines such as those above provide users with knowledge about acceptable and unacceptable online behaviours, and facilitate an orderly trading environment by setting out expectations for both vendors and consumers. Rules are also enforced by cryptomarket administrators and moderators who punish infractions with penalties such as suspension of user accounts. Other common examples of nodal technologies include drug trafficking guides for prospective vendors. These outline various innovative strategies and techniques for concealing illicit drugs so as to confound interdiction by postal inspections regimes (see Chapter 4 for greater discussion of this topic).

Cryptomarket resources

Nodal resources are readily apparent whenever visiting a cryptomarket. For example, physical assets are evident in even the most basic website infrastructure. The presence of an accessible domain name, functional web pages and active discussion forums all indicate tangible resources in the form of operational web servers and computer hard drives. Escrow services similarly demonstrate the existence of

DOI: 10.1057/97811373990520004

Bitcoin or other cryptocurrency 'wallets' which are used to transfer and store digital currencies (Grinberg 2012, Van Hout and Bingham 2013). The total number of users registered to the site is also commonly displayed on the main pages of various cryptomarkets. This information provides observers with a rough indication of the size of nodal membership. Non-physical resources such as programming expertise are reflected in the ongoing maintenance of the programming code that comprises the digital architecture of each site. Programming expertise is also sometimes 'loaned' or 'donated' to cryptomarkets from external parties. For example, in a practice similar to computer hackers who are hired by firms to test their cyber-defences, a user of *Black Market Reloaded* identified and publicised security vulnerabilities on cryptomarket forums:

> It was not our aim to bring BMR [Black Market Reloaded] down, we just published the leak because if we had it, enforcement and private hackers could have it as well, trouble could arise if the leakage would have been exploited without people to know. (Bradbury 2013)

As reflected in the statement above, this hacking attack was carried out not with the intention of stealing information or cryptocurrencies, but rather to identify vulnerabilities and forewarn administrators so that they may fortify their site against attack by genuinely hostile parties such as law enforcement or (other) cybercriminals.

Cryptomarket institutions

Although cryptomarkets operate under strict conditions of anonymity, they are also refreshingly transparent in terms of generic internal organisational structures and divisions of labour. Clearly articulated ranks or positions in the organisational hierarchy are prominently displayed whenever a user posts an announcement or comment on a cryptomarket forum. Also popular amongst various cryptomarkets are 'karma' systems which record and display user information, including the number of successful transactions undertaken and discussion posts made. From these detailed and readily available sources of information, we may deduce four general roles operating across cryptomarkets, including: administrator, moderator, vendor and consumer. Each of these positions comes with its own set of tasks, responsibilities and capacities which are described below.

DOI: 10.1057/9781137399052.0004

Administrators sit at the top of the cryptomarket hierarchy. It is their role to act as executives and formally manage their site, and to determine the policies under which the cryptomarket will operate. In order to execute these tasks, administrators enjoy full access to the cryptomarket, enabling them to perform practically any action, including: authorising and suspending individual accounts; overseeing 'stealth' transactions not publicly listed (see Christin 2013); creating new product categories; authorising or prohibiting the sale of various items; as well as innovating and implementing new security procedures and cyber-defences. Administrators also manage the cryptocurrencies transacted through the cryptomarket. This enables them to accept commissions on any sales conducted through the site or, alternatively, if they are so inclined, defraud users and abscond with any funds waiting in escrow (see, for example, *Sheep Marketplace* Greenberg 2013). An additional role performed by some cryptomarket administrations involves corresponding with media organisations (Greenberg 2013, O'Neill 2013, DeepDotWeb 2014, DeepDotWeb 2014).

Moderators are ranked below administrators in the cryptomarket hierarchy and assist with lower-level site maintenance and customer support. They have limited access to site infrastructure and user information. Their primary tasks involve regulating forum discussions; identifying fraudulent activity committed by scammers and responding to requests for assistance and complaints from vendors and consumers. These positions may attract remuneration from administrators, as is indicated in the job advertisement listed in Figure 1.2.

Vendors use cryptomarkets in order to sell illicit goods. Once registered to a cryptomarket, vendors are able to create and manage their own 'seller page' and begin conducting transactions with consumers.

Consumers purchase goods through a cryptomarket and represent the bulk of registered users. They are able to access various seller pages; purchase goods and provide product feedback; and post messages on discussion forums.

The synergies produced by mentalities, technologies, resources and institutions allow cryptomarkets to function as sites of informal nodal governance. They connect users located all over the world for the purposes of facilitating and regulating black markets involving illicit drugs, as well as other prohibited goods. The fact that cryptomarkets are uncontrolled and unregulated by state or corporate institutions implies (incorrectly) that they are lawless and ungoverned spaces. On

DOI: 10.1057/97811373990520004

Customer support staff needed/job offers

Looking for paid customer support need this:

UPDATE

– some of you are sending me, where they go to school, what past jobs they had and you are verified vendors, ***people, do not do that !*** *I don't want to know where you go to school / past jobs (this is security issue for you, imagine i was not legitimate, don't tell personal details like that). I don't need no personal/specific details, just interested in skills you have. Thanks.*

All must have this knowledge:

– Can use PGP in any way

– Must be smart, honest and good person, willing to help customers

– Verified vendors with spare time are prefered

– Willing to work full time / or be able to provide support like on full time basis

– Will must answer all customer needs/ help customer with orders, find vendors etc..

– Very good computer / internet skills

– html knowledge / editing basic pages is+

– must be able to find informations alone if possible...

Job will be paid weekly with bitcoins, please PM ME your interest and expected salary per month / week.

I would like to take it to new level of service with pandora customer support.

Apply only via PM please.

FIGURE 1.2 *Job advertisement posted on Pandora [accessed 10/2/2014].*

the contrary, as demonstrated in the sections above, cryptomarkets are tightly controlled by well-defined organisational hierarchies. These enforce clearly articulated rules which are developed and discussed by informed users in the context of broader philosophical, political and economic debates.

Community, collective identity and resilience

This final section explores issues concerning community and group identity. The term 'community' is often encountered on cryptomarkets in announcements from administrators, by vendors on seller pages and also by various users in posts on discussion forums. Expressions of community may refer to: people who occupy a specific site (e.g. the

DOI: 10.1057/9781137399052.0004

Pandora community, *Outlaw* community.), the entirety of users populating all cryptomarkets or, alternatively, to the broad collective of dark net users operating on the encrypted TOR network:

> Silk road was for us a very special place and a very special community.
>
> *Vendor post – Silk Road 2.0 forum [accessed 15/5/2014]*

> It's not the vendors or the marketplace that makes a place 'special' in my view – it's the community.
>
> *User post – Pandora forum [accessed 13/4/2014]*

> There have been a lot of improvements since Agora opened so we need toilet the general deep web community know about this.
>
> *User post – Agora forum [accessed 18/5/2014]*

Feelings of community amongst cryptomarket users are not surprising, given the range of common motivations, experiences and circumstances that many are likely to share. These include an interest in and enthusiasm for illicit drug use, as well as hostility towards drug prohibition which, as noted in the previous section, is sometimes grounded in libertarian political ideology. Using a cryptomarket also indicates a minimum level of wealth necessary to own or at least access an internet-enabled computer. These factors point to similarities in social class and levels of education amongst cryptomarket users. Most vendors and consumers are also located in either English-speaking or European countries (Christin 2013), although a range of non-English language cryptomarkets are emerging (DeepDotWeb 2014). This provides further commonalities in terms of largely Western cultural mores and values, and establishes a firm basis upon which specific cryptomarket identities and group norms may develop.

Despite regular references to community and collective solidarity, cryptomarket users express group identity in differing ways. For some, being a member of a cryptomarket community involves embracing and celebrating countercultural, 'outlaw' labels:

> We're a community of criminals, remember, and none of us was new to the dope game when we fired up tor for the first time;)
>
> *User post – Agora forum [accessed 15/5/2014]*

> We're all criminals in one form or another – denial or not. Criminal and proud, fuck a 9 to 5.
>
> *Vendor post – Evolution forum [accessed 15/5/2014]*

DOI: 10.1057/97811373999052.0004

> We are not just criminals we are intellegent dangerouse new age criminals.
>
> *User post – Agora forum [accessed 15/5/2014]*

Other users reject or even reverse this kind of pejorative self-labelling, instead referring to themselves as innovators and freedom fighters, whilst framing the law enforcement agencies that enforce drug prohibition as the 'real' criminals:

> We are not criminals... we're pioneers
>
> *User post – Pandora forum [accessed 13/4/2014]*

> It is a pleasure to be serving alongside the dedicated men and women who continue to fight for our freedom! Keep up the good work everyone!
>
> *User post – Agora forum [accessed 18/5/2014]*

> The police are just a violent gang composed of brutal brainwashed overpaid egomaniac halfwit bullies whose crimes are Officially sanctioned by government and thus are never prosecuted.
>
> *User post – Agora forum [accessed 18/5/2014]*

The comments above are consistent with 'crypto-libertarian' and even 'crypto-anarchist' philosophies that advocate resistance to the state through the use on online encryption technology (May 2001, Curran and Gibson 2013, Karlstrøm 2014). By identifying with these radical perspectives, cryptomarket users are able to justify online illicit trading in the interests of individual liberty and in defiance of perceived heavy-handed and unnecessary state intrusion into the lives of otherwise law-abiding drug users. Personal harms that result from the use of illicit drugs may be dismissed as unfortunate consequences of individuals exercising their legitimate right to freedom of choice, while anti-drug law enforcement is construed as oppressive, militaristic and ultimately counterproductive (see Chapter 4 for further discussion of cryptomarkets and law enforcement).

Membership of a cryptomarket community is not mutually exclusive; many consumers and vendors simultaneously maintain accounts across multiple sites. This allows them to communicate and trade with a broader range of users and facilitates the continuation of online activities in the event that a site is unexpectedly shut down. While users may hold a preference for, or loyalty towards a particular cryptomarket, movement between various sites is not unusual. When users permanently shift membership from one cryptomarket to another, they typically describe

DOI: 10.1057/9781137399052.0004

the process of transfer using language more typically associated with offline global population movements:

> Imigrated couple weeks back... Lets make this a solid, safe and sounding community.
>
> *User post – Agora forum [accessed 18/5/2014]*

> Hi Guys, Were an x SR2 [Silk Road 2.0] Vendor and weve recently migrated to Pandora...
>
> *Vendor post – Pandora forum [accessed 13/4/2014]*

As is the case in the offline world, 'migration' from one space to another may be either voluntary or involuntary. The latter occurs when users are forced to join a new cryptomarket after their home site closes unexpectedly. In instances of involuntary migration, newly arrived users are commonly referred to as 'refugees':

> There are very worrying signs of the times ahead if the new marketplace is to inundated with the refugees.
>
> *User post – Silk Road 2.0 [accessed 15/5/2014]*

> I have to say that I really really like Pandora but lately with all of the refugees, there has been many issues with downtime, timeouts and it has made it impossible for me to conduct business.
>
> *User post – Pandora forum [accessed 13/4/2014]*

> I understand your frustration with the lack of orders but hang in there for a bit. All the sheep and BMR [Black Market Reloaded] refugee's are on their way... Give it a couple weeks, things should get goin here quickly
>
> *User post – Silk Road 2.0 [accessed 15/5/2014]*

The above quotations indicate that cryptomarket refugees are not universally welcomed by users in their newly adopted 'homes', where they are sometimes blamed for increasing the strain on website infrastructure and contributing to longer waiting times for deliveries from favoured vendors. This indicates an intriguing (though far less serious) similarity with the plight of 'real life' refugees, where pejoratively termed 'influxes' or 'inundations' strain local infrastructure and contribute to tension between 'native' and migrant groups. Hostile or negative commentary which stresses the various problems created by cryptomarket refugees is balanced by messages of support from other native users who urge tolerance and respect for recently arrived migrants:

> I welcome refugees from any site.
>
> *User post – Pandora forum [accessed 17/5/2014]*

DOI: 10.1057/97811373990520004

> Thanks for the welcome brothers. I really appreciate it.
>
> *Vendor post – Evolution forum [accessed 17/5/2014]*

> SR [Silk Road] survived they have a tough community which I'm proud to be a part of as well as Agoras.
>
> *User post – Agora forum [accessed 18/5/2014]*

Interestingly, the quotation immediately above refers to *Silk Road* having 'survived', despite the original site being closed down and its alleged administrator, *Dread Pirate Roberts,* arrested. This perspective implies that it is the community of users, rather than the site leadership or infrastructure, which comprises the most important element of a cryptomarket. In the event that a cryptomarket is shut down, the user community is able to persist; users either migrate to other sites or, as in the case of *Silk Road 1.0*, they construct and quickly repopulate a replacement website. The apparent mobility of cryptomarkets users, combined with both site-specific and more general cryptomarket and dark net communal identities, indicates a high degree of interdependence and collective resilience. This facilitates the survival of cryptomarket communities in the face of frequent site closures, regular inter-site migration, hacking attacks and administrator perpetrated frauds, as well as the ever-present threat of arrest posed by law enforcement.

Conclusion

This chapter has explored the multifaceted nature of cryptomarkets to reveal some of the more subtle idiosyncrasies associated with this novel form of online association. To the outside world, cryptomarkets are most easily recognised as manifestations of cybercrime, exploiting new communications and encryption technologies to create vast global networks of offenders. However, these unusual illicit sites are not simply centres of criminal activity. In much the same way that an urban ghetto represents more than a site for the commission of crime, so too does a deeper examination of cryptomarkets reveal more complex and nuanced perspectives. Governing the clandestine activities of cryptomarkets are dynamic and reflexive hierarchies comprising professional executive and specialist personnel. Together, they formulate rules, policies and procedures, articulate and formalise collective aspirations, and also regulate trading activity. Underpinning the successful operation of cryptomarkets are communities of users, including vendors and consumers. These are

DOI: 10.1057/97811373990520004

not passive entities, but rather they represent the engines of cryptomarket activity – debating, rating, buying and selling, and, in the process, shaping their own collective identities. Whilst demonstrably proud and defiant, cryptomarket communities also reveal an acute awareness of their own tenuous foothold in cyberspace. As a precaution against disaster, they maintain close contact with other communities which inhabit the digital frontier, aware that at any moment they and their neighbours could be sharing each other's fate.

Note

1 Direct quotations from cryptomarket posts and announcements often contain spelling mistakes and grammatical errors. Rather than correcting each of these, quotations are presented in their original form.

DOI: 10.1057/97811373990520004

2
Cryptomarket Operations

Abstract: *Chapter 2 explores how cryptomarkets operate from a commercial perspective. The processes involved with the buying and selling of illicit drugs online are outlined, as are the significant benefits available to both vendors and consumers who trade drugs online. Website and vendor-specific branding and marketing strategies are discussed, revealing a remarkable degree of convergence with approaches employed by businesses in the legitimate economy. User feedback and automated ranking systems are also discussed as critical to the success of cryptomarkets.*

Martin, James. *Drugs On the Dark Net: How Cryptomarkets Are Transforming the Global Trade in Illicit Drugs*. Basingstoke: Palgrave Macmillan, 2014. DOI: 10.1057/9781137399052.0005.

In addition to constituting sites for the commission of cybercrime and nodal governance, cryptomarkets are also sophisticated trading entities and hubs of commercial innovation. In this context, their primary functions are to attract users and facilitate the exchange of illicit drugs in an expanding and increasingly competitive online marketplace. The development of cryptomarkets is therefore shaped not only by encryption technology and the threats posed by law enforcement, but also by the needs and preferences of their clientele. In order to address these, cryptomarkets employ a user-friendly interface, the operations of which are underpinned by a generic structure derived from the archetypal illicit drug site *Silk Road 1.0*. Cryptomarkets therefore have a range of common features, including the division of each site into various product categories and vendor sub-pages; photographs of products and the use of vendor and product-specific marketing strategies; and the availability of user-generated feedback and automated ranking systems.

The broad similarity between cryptomarkets enables users the convenience of switching seamlessly between various sites without the need to learn a new system of operations. From a scholarly perspective, it also facilitates comparative analysis and enables academics to trace the ongoing evolution of cryptomarkets as various sites expand, innovate and include new services into their repertoire. While cryptomarkets have a range of commonalities, each site also manifests its own idiosyncrasies, stylistic conventions and features. These are necessary in to order differentiate each site from its competitors, allowing it to attract new and repeat users and, if a new addition to the dark net, establish a foothold as an illicit trading nexus. Areas of innovation include novel security features intended to safeguard against penetration by hackers and law enforcement, and the provision of advanced customer services, including multi-lingual technical support available across a range of time zones.

This chapter explores the ongoing evolution of cryptomarkets from the perspective of those who use these sites to trade illicit drugs. Of particular importance is how cryptomarkets carry out everyday operations and respond to the unique challenges associated with online illicit trading. The basic purchasing process and feedback systems are analysed, as are the various marketing strategies employed by both cryptomarket administrators and individual drug vendors. In seeking to understand cryptomarkets as commercial enterprises this chapter aims to determine new information about the nature of illicit online trading and shed further light on the users of these sites.

DOI: 10.1057/9781137399052.0005

Challenges facing users of cryptomarkets

As anonymous, virtual and illicit trading forums, cryptomarkets face a range of challenges in attracting clientele and convincing both buyers and sellers of the reliability of their services. Some of the obstacles which undermine consumer trust in cryptomarkets are relatively well understood because they are common to other, legal online shopping websites. For example, customers shopping online are unable to physically enter a store and interact face-to-face with reassuring salespeople; they may not inspect or sample goods before purchasing; there are no accessible locations where products may be returned or complaints lodged; and online shoppers cannot insist on 'seeing the manager' and making their physical presence felt if the consumer experience is not up to their satisfaction. Research from the business and marketing disciplines indicates that the unfamiliarity and distance associated with online retailing leaves potential customers feeling vulnerable, untrusting and hesitant in departing with their hard-earned funds (Chen and Dibb 2010, Rose, Hair et al. 2011). This means that people seeking to sell drugs through cryptomarkets are, like other online retailers, distanced from prospective customers to such an extent that establishing a productive and sufficiently trusting relationship can be highly problematic.

Cryptomarkets in particular arouse further mistrust amongst potential users due to an almost total absence of external regulation. Unlike online businesses that operate in the legitimate economy, cryptomarkets (and other black market industries) are not subject to state monitoring or oversight. Products that are sold on illicit sites bypass the processes of government-mandated testing, quality control and safety standardisation that are imposed on regular consumer goods. Assurances of quality for various products are also unable to be verified by the usual range of commercial and non-government organisations, such as product reviewers and consumer advocates. The news media, traditionally another important source of consumer information, have so far played only a minor role in reporting quality of service issues and scams carried out via cryptomarkets (Foxton 2013, Moses 2013). Much of the reporting regarding cryptomarkets (and also crime more generally) is undermined by sensationalist or erroneous claims, for example, that *Silk Road 1.0* dealt in child pornography or 'hitman' services (Flitter 2013, Rubens 2013). Inaccurate reporting such as this damages the credibility of the news media and, from a consumer perspective, undermines the usefulness

DOI: 10.1057/9781137399052.0005

of this sector as a reliable source of information about the online illicit drugs trade.

The absence of oversight and commentary from those state and non-state institutions that assist with regulating the legitimate economy leaves consumers who are considering making a purchase on a cryptomarket with a high degree of uncertainty regarding the quality and reliability of products and services that are available. This unease is compounded further by a lack of external recourse and arbitration mechanisms, such as state-funded corporate watchdogs, ombudsmen and small-claims courts that are usually on hand to enforce trading laws and resolve disputes. With no formal, state-sanctioned processes guaranteeing conditions or terms of sale, and in the absence of any external avenues of recourse, both buyers and sellers who use cryptomarkets face the uncomfortable prospect that if something goes wrong with an online transaction then they are effectively 'on their own'. Users of cryptomarkets are therefore exceptionally vulnerable to online sellers who spruik sub-standard goods or services, and to scammers seeking to exploit the lack of regulatory oversight and conduct bogus transactions.

Perhaps the single greatest obstacle to people considering using a cryptomarket, however, is the risk of their online anonymity being comprised and their identities revealed to law enforcement. As is the case with all black markets, the usual role of the state as regulator and protector is inverted, as law enforcement agencies seek to track down and prosecute both buyers and sellers alike. The threat posed by law enforcement places a significant burden on the administrators of cryptomarkets who must somehow convince potential clients that using their services will not result in arrest and incarceration. These are not minor concerns given the illegal and highly controversial nature of many of the products that are routinely traded via cryptomarkets, particularly illicit drugs. As is routinely publicly stated by law enforcement representatives, people who buy or sell prohibited goods online face the very real prospect of arrest and, depending on the severity of the offence, "maximum penalties of life imprisonment" (AFP 2012) if investigators are able to determine their identity and location (FBI 2013, DEA 2014, FBI 2014).

Encrypted identities are vulnerable to being exposed at various points in the online transaction process. These include during product delivery, if consignments of illicit goods are improperly concealed or fall foul of random or targeted inspection by customs or postal agencies (see Chapter 4 for more detailed discussion of law enforcement and

DOI: 10.1057/9781137399052.0005

cryptomarkets). Alternatively, cyber investigators may uncover the identities of illicit traders through infiltrating the networks of cryptomarket administrators. This is a particularly worrying prospect for users due to the potential for detection long after an illicit transaction has been undertaken. Recently publicised arrests in the United States, Britain and Australia following the closure of *Silk Road 1.0* highlight the persistent threat posed by incriminating 'digital fingerprints' that linger in cyberspace or on seized hard drives even after a cryptomarket has been taken offline (Kerr 2013, Ross 2013). Despite their relative infrequency, high-profile arrests such as these are likely to produce a significant deterrent effect, dissuading potential online buyers and sellers from engaging in cryptomarket transactions.

At the more conspiratorial end of the range of perceived threats to online anonymity are so-called honey pot theories. Proponents of these claim that particular online vendors or entire cryptomarkets are fronts for law enforcement that have been set up in order to entrap unwitting buyers and sellers (Greenberg 2013). More extreme variants of the honey pot theory suggest that TOR encryption was established with deliberate security vulnerabilities or 'back doors' which permit external monitoring (Ball, Schneier et al. 2013, Schneier 2013). Some of these ideas bear the hallmarks of a classic conspiracy theory. However, given the (well-documented) role of the US military in establishing the TOR network (Dingledine, Mathewson et al. 2004), as well as recent revelations about the colossal online surveillance programs currently being undertaken by the US National Security Agency and allied '5 Eye' intelligence organisations (Ball, Schneier et al. 2013, Schneier 2013), concerns that at first glance may seem paranoid or delusional are perhaps not quite so easy to dismiss as they once might have been.

Some of the threats associated with using cryptomarkets appear more credible and imminent than others. However, gauging the veracity of any of them beyond a vague impression is extraordinarily difficult. Cryptomarket technology is new, highly complex and is constantly being updated, challenged and reinforced, as cyber investigators and their targets evolve and adapt to developments online. Sources of accurate, impartial and up-to-date information about this ongoing struggle and the 'true' vulnerability of cryptomarkets to penetration by law enforcement are scarce. Understandably, law enforcement agencies generally remain tight-lipped about the limits of their investigative capabilities. This is possibly because they wish to avoid compromising ongoing

DOI: 10.1057/9781137399052.0005

investigations, or alternatively, as some online security experts suggest, because they are relatively underdeveloped and currently pose a minimal threat to users of cryptomarkets who are scrupulous in protecting their online anonymity (Moses 2013).

While law enforcement agencies may be tempted to exaggerate their powers of detection, administrators of cryptomarkets (whether genuine or honey pot) have a vested interest in 'talking up' the levels of security protecting their users in order to attract additional business. This suggests that both sides of the cryptomarket phenomena (i.e. cryptomarket administrators and law enforcement agencies) have an incentive to provide minimal or even potentially misleading information to the broader public about the risks associated with online illicit trading. In the absence of impartial sources of information, and with no long-term, cyber-policing/cryptomarket trends available to provide historical context, determining even general levels for risk for buyers and sellers using cryptomarkets is, for the time being, practically impossible.

What is clear, however, is that there is an extensive list of both real and perceived threats associated with the use of cryptomarkets. Given the relatively paucity of information available with which to assess their levels of seriousness, and the potentially disastrous consequences of online transactions that end badly or are detected by legal authorities – ranging from a simple loss of funds to decades of imprisonment – it may seem surprising that cryptomarkets attract any users at all. The fact that they do, and indeed appear to be steadily proliferating, testifies to the ubiquity and strength of demand for illicit goods and services that are available online. It also suggests that cryptomarket administrators are achieving at least some success in addressing the concerns of their users, many of whom could presumably source or sell illicit goods using more conventional methods.

The buying and selling process

Drug distributors and other illicit traders who wish to sell goods or services though a cryptomarket must first identify and access a suitable site, and then register as a vendor. At a minimum, this involves paying a one-off registration fee (usually ranging between USD $200 and 300) to the site administrator, which enables the vendor to create an account into which Bitcoins or other cryptocurrencies may be accepted. Once

DOI: 10.1057/9781137399052.0005

the registration process is complete, the vendor is able to create their own 'seller page'. A vendor's seller page is essentially their online storefront; it contains all of the information about themselves that the vendor wishes to publicise to potential customers, as well as the products and services that they have listed for sale. Basic information that is necessarily displayed on a seller page includes the range and prices of the various goods on offer and the quantities in which they are sold (e.g. by the gram, ounce, or total number of pills). The geographical locations to which goods are able to be delivered are also listed, with some vendors opting to sell solely to a domestic customer base, while others are prepared to send goods internationally. Product prices and packages that are listed on a seller page are pre-determined by the vendor, rather than through customer bidding of the type seen on legitimate online marketplaces such as eBay.

Consumers seeking to purchase goods or services through a cryptomarket must also create a (free) buyer account from which cryptocurrencies may be transferred. They are then able to browse through the cryptomarket in much the same way as any legitimate commercial website, selecting different product categories (e.g. cocaine, ecstasy, cannabis), accessing various seller pages and comparing the different purchasing options that are on offer. When a consumer finds a product that they wish to purchase they may then begin the process of cryptocurrency exchange. There are two methods through which funds may be exchanged on a cryptomarket: 1) in escrow until product delivery, meaning that monies are held by the cryptomarket administrator and are not transferred to the vendor until the consumer authorises final payment; or 2) the customer may 'finalise early' (FE) and transfer funds immediately upon purchase. Goods that have been purchased are then sent directly from the vendor to the consumer via conventional postal networks. Consumer feedback is the final optional stage in the transaction process and involves customers providing ratings and comments regarding the quality of purchased products and the overall level of service provided. This feedback is then posted on the vendor's seller page and is made visible to other prospective customers.

The use of escrow is one aspect of the buying and selling process that has changed significantly since the closure of *Silk Road 1.0*. Customers who traded on early cryptomarkets were regularly advised to rely on escrow as a guard against potential scammers who may be posing as legitimate online drug vendors. While the use of escrow appeared

DOI: 10.1057/97811373990520005

effective in minimising instances of vendor-customer fraud, its widespread utilisation resulted in other problems. The larger a cryptomarket grows, the more funds the administrator is likely to hold in escrow. Large amounts of difficult to trace cryptocurrencies are a valuable target for both external hackers, as well as for cryptomarket administrators tempted to abscond with their users' funds. A number of cryptomarkets have been closed in recent months after millions of dollars in user funds waiting in escrow accounts had been stolen either by external hackers or by cryptomarket administrators.

Vendor registration, security and cryptomarket branding

The basic process of buying and selling products on cryptomarkets is relatively generic and varies little between different sites. However, each of the apparently simple steps involved with a cryptomarket transaction conceals a host of more complex processes and functions. In the first instance, the initial stage of vendor registration offers cryptomarket administrators the opportunity to enhance site security and differentiate their cryptomarket from competitor sites. On many earlier cryptomarkets, such as *Silk Road 1.0* and *Black Market Reloaded*, payment of the vendor registration fee was all that required for a seller to create an account and begin the online trading process. Newer and more security conscious cryptomarkets, however, have begun imposing additional barriers to vendor registration. *TorMarket*, for example, accepts new vendors only by invitation. Invitees must have a "flawless" record of sale already established on other cryptomarkets, and also demonstrate that they employ sufficiently sophisticated postal concealment or 'stealth' techniques, such as printed labels and vacuum sealed or moisture barrier bags (see Chapter 4 for more about counter-interdiction techniques and strategies).

Additional obstacles to vendor registration may improve site security, but they also come with significant costs. A more stringent registration process means that the overall number of vendors who are able to register on the site is inevitably lower than it would be under a more open system. This has flow-on effects, including limiting the range of goods and services that are available, and reducing the level of competition between vendors. The fact that some newer cryptomarkets are prepared

DOI: 10.1057/9781137399052.0005

to make this trade-off – eschewing range and openness in favour of enhanced security – speaks to the more cautious online illicit trading environment that has emerged in the wake of several high-profile cryptomarket closures, particularly those of *Silk Road 1.0*, *Black Market Reloaded* and *Sheep Marketplace*. A likely consequence of these closures, as well as the arrests and loss of funds that accompanied them, is that both vendors and consumers now place an even greater premium on measures that ensure anonymity and secure encryption than they had in the past.

Increased caution and security consciousness amongst users is reflected in changes to how cryptomarkets implement and advertise site encryption and other security-related measures. On early cryptomarkets, such as *Silk Road 1.0*, internal security was relatively lax and the website programming code has been criticised as flawed (Leger 2014). Despite undertakings on behalf of administrators to regulate the site, responsibility for safe trading was ultimately placed with users:

> [We] hold our members to the highest standards of personal conduct and work tirelessly to prevent, root out and stop any scammers that may try to prey upon others. However, the best way to stay safe and make sure your experiences here are enjoyable is to educate yourself on how Silk Road works, and take advantage of all the tools and guidelines we have made for you.
>
> *Excerpt from welcome message – Silk Road 1.0 [accessed 31/5/2012]*

Reminders of *caveat emptor* and calls for users to conduct due diligence contrast significantly with the slick, security-related, marketing-style messages that users first encounter when accessing newer cryptomarkets such as *TorMarket*. On this site, users are greeted with a professional looking welcome page, complete with corporate logo and prominent messages about enhanced security measures ('Only Encrypted Addresses', 'Built in Bitcoin Mixer', 'Trusted Vendors Only', etc.). Additional security innovations that are under development are also advertised ('PGP Auth [coming] soon') alongside guarantees of 'VIP Support' ('We mark and handle all your messages with the utmost priority'). Even the *TorMarket* tagline– *'[The] Darknet Market done right: Secure codebase, competent operators, and common sense'* – exudes a sense of cool professionalism that is at odds with the more intimate and folksy tone that was characteristic of earlier cryptomarkets. It also implies criticism of other sites presumably managed by less competent and responsible parties.[1]

DOI: 10.1057/9781137399052.0005

The prominence of messages spruiking enhanced site security and tough vendor registration requirements suggests that these innovations serve two related functions. While ostensibly intended to secure cryptomarkets against infiltration by law enforcement and scammers, they also provide timely reassurance to prospective vendors and customers who may have been spooked by recent cryptomarket closures. In this regard, security measures transcend their instrumental functions, and become a means by which site administrators can help re-establish trust between vendors and consumers and restore confidence in cryptomarket trading. An explicit commitment to enhanced security also affords site administrators the opportunity to differentiate their cryptomarket from those of competitors and to establish an independent, reputable and trusted 'brand'. Given the multiplicity of cryptomarkets that have emerged following the closure of *Silk Road 1.0,* and the inability of any single site to establish the same level of market dominance, any measures that enhance a site's competitive profile are likely to be vigorously pursued, implemented and publicised in any way possible.

Due to the fact that cryptomarkets deal in illicit goods and services they are, naturally, unable to employ traditional forms of commercial advertising. This means that new cryptomarkets seeking to break into the illicit online market must find alternative ways to spruik their services and establish brand awareness. This is another area in which administrators of cryptomarkets have demonstrated considerable innovation. For example, following the 2013 launch of the cryptomarket *Atlantis*, its administrators released a promotional video on *YouTube*, advertising the site as "the world's best anonymous online drug marketplace", and outlining a range of unique benefits available in comparison to its competitors, including no sign up fees and free product delivery (Quigley 2013). The video was initially posted on the 23rd of June 2013 (which is, ironically, also the date designated by the UN as the annual 'International Day Against Drug Abuse and Illicit Trafficking') and attracted some 50,000 views, as well as being reposted on a variety of other technology news sites before it was eventually removed by *YouTube* moderators. According to an (encrypted) public statement released by *Atlantis* co-founder 'Loera', "the commercial was a great success" and assisted the cryptomarket in securing over $1 million USD in sales (Loera cited in O'Neill 2013).

The extraordinary world-wide media attention that followed the *Atlantis YouTube* advertisement contrasts significantly with more recent and conspicuously lower-key cryptomarket 'launches'. The administrators of

DOI: 10.1057/9781137399052.0005

Outlaw, for example, helped promote their site by conducting an interview with journalists at *DeepDotWeb*, a technology website specialising in cryptomarket news (DeepDotWeb 2014). As part of the interview, the *Outlaw* spokesperson articulated their vision for the site and outlined new security features and services. While the interview attracted no further press coverage, it is arguably a much more effective and mutually beneficial promotional tool than utilising non-specialist forums such as *YouTube*. *Outlaw* administrators were able to publicise detailed information on a forum of particular interest to their likely customer base, while *DeepDotWeb* was able to also secure a significant media 'scoop'. Perhaps most importantly, exposure was limited to those with a pre-existing interest in cryptomarket news. This allowed *Outlaw* administrators the greatest opportunity to reach potential customers without attracting unnecessary attention from either the broader public or from law enforcement.

Seller pages and vendor branding

Just as various site innovations are employed in order to help differentiate one cryptomarket from another, customisable seller pages also allow individual vendors the opportunity to establish a direct relationship with customers and create their own sub-brand within a cryptomarket. This vendor-level branding is achieved via a number of different methods. Firstly, the vendor's choice of name may tap into or communicate ideas that appeal to certain types of customers. For example, vendor names often reference particular illicit drugs or aspects of drug culture (e.g. 'cannabis connection', 'Dr Leary'). Names related to drug-themed television shows such as *Breaking Bad* are particularly popular, (e.g. 'haizenberg', MrWhiteInc,), as are those linked to geographical locations that are associated with drug production/consumption (e.g. 'holland online', 'Czechlab'). Some vendor names are overtly humorous ('Nancy Reagan', 'ReDEyEsEmporiuM'), while others reflect a more professional tone that is reminiscent of conventional corporate branding and sloganeering (e.g. 'Platinum Standard', 'Refresh Yourself', 'synthetics r us').

Pictures and logos hosted on seller pages are used to further construct a sense of vendor identity and to build brand awareness, as well as to advertise particular products, (e.g. photos of lush marijuana buds, or piles of brightly coloured ecstasy pills). Symbols of subversion are also

DOI: 10.1057/97811373990520005

popular in the background of these for photos, particularly people wearing 'Anonymous-style', Guy Fawkes masks. The quality and sophistication of photographic advertisements images varies widely, from poor resolution to high-grade, professional looking photos that would look at home (aside from the content) on a conventional commercial website. This level of contrast in terms of quality is similarly reflected in the text-based information that is provided by vendors. While some seller pages display very limited, grammatically incorrect, poorly spelled or profanity-filled welcome messages and product descriptions, others are relatively well crafted. Indeed, many of the more successful and reputable cryptomarket vendors use phrases and commercial jargon that bear a striking resemblance to those used in the legitimate retailing sector.

Examples of typical marketing-style rhetoric hosted on seller pages include mission statements and organisational goals, as well as undertakings to provide the highest possible levels of customer service, and to respond to user concerns or complaints with the greatest possible haste and efficiency:

> ==========Top quality product & friendly service ==========
>
> We are a group of experienced top 10% vendors from SR1.0 ...
> We strive to give you a safe, reliable and professional delivery service ...
> Don't take our word for it. Try our service and experience the ease yourself ...
>
> Why you should try our service:
>
> ☐ High quality product for a good price
> ☐ Friendly communication & timely order updates
> ☐ We offer a reliable & safe service (thousands of satisfied customers on SR)
> ☐ Returning customers get discounts and you always get extra samples!
>
> *Excerpt from seller page – Silk Road 2.0 [accessed 23/12/2013]*

- *We stand for the best MDMA products such as pills and pure MDMA Crystal.*
- *We carry the strongest and most exotic Mdma-pills around so no need to look further your at the right place!*
- *As for shipping service we use the most safe methods for packing and sending your order no matter how big or small.*
- *Fast and clear communication, top notch service & product is what we deliver*

Excerpt from seller page – Silk Road 1.0 [accessed 10/12/2012]

DOI: 10.1057/9781137399052.0005

The excerpts above are representative of the generally welcoming and professional tone that is characteristic of vendor-customer communications provided on seller pages. They are also strongly reminiscent of conventional retail sloganeering of the legitimate corporate sector. The tone and content of these messages contrast significantly with the communication styles stereotypically associated with conventional drug dealers, and are likely to strike a reassuring chord amongst consumers who are accustomed to high levels of retail service in other aspects of their lives. This contributes to the overall quality of the 'consumer experience' encountered on cryptomarkets and helps account for the extraordinarily high levels of customer satisfaction reported by cryptomarket users (Christin 2013, Hout and Bingham 2013).

Product differentiation, marketing and sales

Similarities between conventional and cryptomarket retailing techniques are further reflected in how vendors promote individual products and use gimmicks to attract new and repeat customers. Notable amongst these are periodic lotteries for free illicit drugs or cryptocurrencies (e.g. '1 YEAR ANNIVERSARY GIVEAWAY! 250 BTC!!!'; 'POWERBALL Lotto LAUNCHED! *Massive Jackpot!*'), reward programs for repeat customers and discounts for holidays or special events such as Halloween and New Year's Eve. On occasion, cryptomarket administrators may also collaborate with vendors to actively support promotional activities. For example, on 'Pot Day' (4th of April) 2012, *Silk Road 1.0* administrator *Dread Pirate Roberts* joined with vendors offering discounts for cannabis products, waiving all daily commissions usually charged on sales conducted through the site (Ormsby 2012).

While gimmicks and promotional activities are commonplace on cryptomarkets, there are other, perhaps more important, measures that are employed by vendors in their efforts to make sales and ensure product turnover. These include competitive pricing, claims to quality and a range of different purchasing options (e.g. discounts for bulk purchasing). As one might expect, many vendors express a commitment to selling only the finest, highest-purity, 'lab-tested' products available. Sometimes claims to superior quality are supported with additional information, such as reports showing detailed chemical analysis of particular products or photographs of recently completed drug testing kits. This

DOI: 10.1057/9781137399052.0005

supplementary information, if accurate, provides online consumers with a level of knowledge regarding the composition and potency of illicit drugs that far exceeds that typically available when sourcing drugs from conventional markets.

Interestingly, not all vendors claim to sell exclusively high-quality goods and instead offer a variety of products ranging from superior and relatively expensive to cheaper and explicitly lower quality. Many cocaine vendors, for example, distinguish between 'pure' or 'high-grade' and 'sociable' cocaine, with the two differently priced products marketed towards the same clientele but apparently intended for use in different settings (i.e. for personal use or sharing on social occasions). Other vendors cater exclusively to a more price-restricted customer base and are often remarkably up-front regarding the relatively poor quality of the goods listed for sale:

> Hey Guys, We have some good quality coke here perfect for social events when you have a budget!
>
> We do not claim this is top quality flake 90%, its lower quality reaching about 65% purity which is better then street and about the same price.
>
> *Excerpt from seller page – Pandora [accessed 4/1/2014]*

Given the immediacy and prominence of consumer feedback (see section below), vendors who advertise lower quality products may simply be acting in their own interest in pre-empting negative comments and managing the expectations of customers who are both well-informed and have the option of buying from a range of different suppliers. However, different product qualities and pricing categories also afford customers a wider degree of choice and flexibility when considering their many purchasing options. This is beneficial for consumers who may wish to purchase drugs that are explicitly cheaper and lower quality. For consumers of illicit drugs, the range of options that is available through cryptomarkets compares favourably with the relatively limited alternatives available through conventional drug markets (Hout and Bingham 2013). Instead of being forced to rely on social networks or contacts made spontaneously at sites of drug consumption (e.g. nightclubs, music festivals), online drug shoppers are empowered with a high degree of information and an unprecedented range of competitively priced goods. From a consumer perspective, this makes purchasing illicit drugs online more similar to shopping experiences in the legitimate economy, where retailers employ competitive pricing, a diverse range of products and high levels of customer service to actively attract consumers.

DOI: 10.1057/9781137399052.0005

In some instances, the level of corporate mimicry and marketing rhetoric displayed on cryptomarkets borders on the bizarre. For example, one *Silk Road 1.0* vendor, following a detailed mission statement and 'oath to customers', also claimed to be a "Proud financial supporter of Wikileaks & Bluelight". At first glance, a vendor spruiking their social conscience through corporate-style sponsorship may seem at odds with what one may expect from someone who is engaged in transnational drug distribution. However, the choice of organisations that this vendor claims to support – a subversive, anti-state, information and internet freedom advocate, and an illicit drugs information and harm reduction centre – fits well with the likely profile of cryptomarket users who, presumably, must be minimally internet savvy, share some disregard for state prohibition laws, and are likely to have a vested interest in safe drug use.

A range of similarly innovative and seemingly incongruous approaches to vendor branding are also employed across a variety of cryptomarkets. These include a commitment to the use and sale of 'organic' ingredients and products, including opium and marijuana. Even more striking are advertisements from vendors who claim to source products ethically, for example, selling cocaine that has been purchased directly from agrarian workers rather than notoriously violent drug cartels:

> We are a team of libertarian cocaine dealers.
> We never buy coke from cartels!
> We never buy coke from police!
> We help farmers from Peru, Bolivia and some chemistry students in Brazil, Paraguay and Argentina.
> We do fair trade!
>
> *Excerpt from seller page – Evolution [accessed 28/12/2013]*

> This is the best opium you will try, by purchasing this you are supporting local farmers in the hills of Guatemala and you are not financing violent drug cartels.
>
> *Excerpt from seller page – Evolution [accessed 28/3/2014]*

Descriptions such as 'conflict free', 'organic' and 'fair trade' are, obviously, impossible to verify on a cryptomarket. The processes involved with certifying products in this manner are sufficiently difficult in the legal economy, let alone amongst distributors of black market goods who by necessity must conceal critical elements of the supply chain. However, the fact that some cryptomarket vendors believe that ethical dimensions of drug production and supply and broader notions of social responsibility are important to their customers is, in itself, intriguing on

DOI: 10.1057/9781137399052.0005

a number of levels. Firstly, the use of ethical labelling runs contrary to impressions of ruthless drug retailers and haplessly addicted consumers that are routinely propagated by the state and in the news media. The fact that ethical marketing strategies are being used on cryptomarkets is an indicator that some consumers are highly discerning, considering issues such as social responsibility, along with other factors such as price and quality, when considering their purchasing options.

Secondly, in employing ethical marketing strategies online drug vendors are explicitly differentiating themselves from the conventional illicit drugs trade and its historical association with violence and exploitation. This attempt to promote a positive and socially responsible image of online illicit drug trading is consistent with the (generally) violence-free ethos and operation of cryptomarkets, which minimises conflict through the geographical separation of trading partners, and by providing escrow services and online forums for dispute resolution. While sourcing illicit drugs from ethical suppliers does not appear to be feasible, at least not in any verifiable sense, it should come as little surprise that these initiatives are both the subject of discussion in cryptomarket forums as well as being pursued by cryptomarket vendors.

Finally, in claiming to fund social activism and harm reduction organisations, and in apparently embracing a 'fair trade' style business model, online drug distributors reveal a remarkable degree of convergence in marketing strategies between licit and illicit commercial entities when permitted by broader market conditions. This convergence would not be possible in the conventional illicit drugs industry as violence (or at least the threat of violence) is necessary in order to ensure security and deter predation from rival criminal groups. In this context, promoting one's drug distribution organisation as concerned with ethical behaviour, social responsibility and broader notions of progressive idealism is likely to run contrary to the essential task of maintaining a fearsome reputation. In an anonymous online trading environment, however, the need to maintain a violent deterrent vanishes, and drug distributors are free to create a more socially constructive public image that is both free from violence and more attuned to the perceived priorities of their customer base.

Customer feedback and seller rankings

Perhaps the most important feature common to all high-profile cryptomarkets, including *Silk Roads 1.0* and *2.0*, *BMR* and *Sheep Marketplace*,

DOI: 10.1057/9781137399052.0005

is user feedback. All customers who purchase goods through these sites are encouraged by the site administrators to provide publicly available information regarding the quality of the goods or services that have been purchased. Customer feedback takes a variety of forms, ranging from detailed comments about shipping times, 'stealth' measures and the perceived potency of illicit drugs, to a simple 5-star rating (see Figures 1.1 and 1.2). In many instances, feedback provided in this manner is uploaded to a vendor's seller page as soon as transactions are completed and goods are received. This allows prospective customers 'fresh', up-to-date information not only about the recent performance of various vendors, but also about individual batches of illicit drugs that may still be available for purchase.

rating	**review**	**freshness**
5 of 5	FE, I'm liking the feedback.	FE, I'm liking the feedback.
5 of 5	FE early cuz of my low order count. Trust this vendor per forums. Peace	13 hours
5 of 5	lush pills, really hit the spot thank you.	1 day
5 of 5	Great Vendor 2nd Order To Uk, Fast Dispatch..Few Days To Your Door, Be Back After The Weekend..Thanks Again.	1 day
5 of 5	5/5 very stealth & fast; shipping! (3 days around europe) product as described.	1 day
5 of 5	fast delivery again and even better packaging A +++	1 day
5 of 5	super fast delivery, great looking and smelling pills!	1 day
5 of 5	Delivered 2 days after ordering to Germany, Extremely clever packaging. Will order again	1 day
5 of 5	Awesome.....!!!!!	2 days
5 of 5	FE for trusted seller. Prompt customer service. Very hopeful it will arrive. Thanks guys	2 days

FIGURE 2.1 *Customer feedback page – Silk Road 1.0 [accessed 15/12/2012]*

Feedback from customers may be supplemented with additional information that is provided independently by the website administrator, such as the number of transactions that the vendor has successfully completed (or failed to complete), and the total value of goods that they have traded. Data that are compiled in this way are processed automatically by cryptomarket administrators in order to rank vendors according to their perceived reliability and their relative levels of performance and customer satisfaction.

DOI: 10.1057/9781137399052.0005

The availability of information such as automated seller rankings means that whenever a prospective customer logs on to a cryptomarket and selects any given product or service category, the full range of registered vendors are displayed, with those 'most trusted' (i.e. those with best records of customer feedback) listed at the top of the page, and those ranked poorly with either predominantly negative reviews or with no established record of transactions displayed at the bottom.

Importantly, unlike other information that may be volunteered on a seller page, vendors are not able to alter or remove feedback that is provided by customers. This means that product reviews, whether positive or negative, are always posted to the vendor's seller page and remain permanently visible in their record of transactions. The fact that vendors are unable to directly control what feedback is published on their pages lends much-needed credibility to otherwise unverifiable information about the quality and reliability of goods and services that are available. Permanently recorded customer feedback also contributes to a remarkable degree of sensitivity to negative ratings and comments on the part of many vendors. The following excerpts from seller pages are typical of the sentiments expressed by cryptomarket vendors about the importance of positive customer feedback:

> Understand that your Feedback is the foundation of our business... If you have ANY problems, please contact us before giving us a bad rating. In 99% of the cases we are able to satisfy you! Please leave also your honest feedback, to help following buyers get an opinion about us :)
>
> *Excerpt from seller page – Tormarket [accessed 11/12/2013]*

> Seller reputation is everything in a market like this, and we strive for 5/5. That can only be provided by you, the buyer. Make sure that you provide feedback for EVERY ORDER. If, for whatever reason, you are unsatisfied with your purchase, contact us immediately (BEFORE YOU POST FEEDBACK) so we can ensure your satisfaction.
>
> *Excerpt from seller page – Silk Road 1.0 [accessed 10/12/2012]*

> We are here to serve our customers in the best way we can, providing the highest quality products and customer service. Every suggestions are more than welcomed since it may improve our business. If you are not satisfied with the product, customer service or delivery please contact use BEFORE you give a negative feedback / low rating. I'm sure we can work it out. As a vendor, reputation is very important to us!
>
> *Excerpt from seller page – Tormarket [accessed 11/12/2013]*

DOI: 10.1057/9781137399052.0005

Given the large numbers of vendors that may be registered under any given category (*Silk Road 1.0*, for example, had over one thousand registered vendors with more than twenty thousand products listed under each of the popular categories, such as cannabis, ecstasy and cocaine), and the dearth of independent, verifiable product and vendor information, customer feedback and automated seller rankings have a significant influence on the purchasing decisions of people using cryptomarkets. The importance of the online reputation of vendors, as expressed through customer feedback and seller rankings, is supported by both ethnographic (Hout and Bingham 2013) as well as quantitative research (Christin 2013).

By empowering customers with up-to-date, accessible and easily comparable information, the customer feedback system facilitates a more transparent and competitive online trading environment. Those vendors who establish a record of reliability and high-quality service are able to use their enhanced reputation and high seller ranking to attract additional business. This provides additional opportunities to interact with new and repeat customers and create further business. Conversely, vendors who sell inferior products or who defraud their customers quickly attract public censure and their business suffers accordingly. According to drug researchers Hout and Bingham (2013), consumers who use cryptomarkets are remarkably savvy about interpreting each other's feedback and place great importance on recent comments when making purchasing decisions.

Challenges associated with online reputation and user feedback

User feedback is vital to the successful operation of cryptomarkets and affords consumers important information about the quality and reliability of the goods and services that are available to them. Despite this utility, however, vendor reputation and user feedback systems also produce a range of outcomes that are unlikely to have been intended when they were first implemented. Firstly, the prominence of user feedback and automated rankings may result in over reliance of consumers on trusted sellers with demonstrated records of success to the detriment of new vendors entering the market. On *Silk Road 1.0*, for example, out of a total of 1239 registered vendors, a small group of approximately only

DOI: 10.1057/9781137399052.0005

100 accounted for 60% of transactions recorded over a six-month period (Christin 2013). This tendency for consumers to rely on well-established vendors is understandable considering the potential for scams and other negative transaction outcomes. Given the relatively wide range of products still available within a limited pool of highly ranked sellers, there is little need for a consumer to take the risk of purchasing from a relatively unknown and untested vendor. This means that new vendors may find themselves 'locked out' of established cryptomarkets, despite a desire and willingness to sell high-quality products.

New vendors who are unable to 'legitimately' establish themselves on a cryptomarket may seek to exploit another weakness associated with the feedback system: its vulnerability to potential 'gaming'. As neither real names nor addresses are recorded when creating a cryptomarket account, there is little to stop dishonest and opportunistic vendors from creating their own customer accounts in order to generate 'dummy' transactions. These essentially allow vendors to sell products back to themselves, creating an opportunity whereby they can write deceptively positive, self-generated reviews. Indeed, recent comments made by an online vendor suggest that this practice is widespread and, to a degree, expected and even tolerated (O'Neill 2014). In addition to creating false positive reviews, unfairly negative customer feedback can also be misused in order to damage the reputation of other vendors. Rival vendors may be motivated to write false negative reviews in order to damage the business of competitors and secure an unfair advantage. The possibility for user feedback to be misused in this manner points to the difficulty in verifying information in an online environment where anonymity is paramount.

The customer feedback systems employed by cryptomarkets are not original innovations. Rather, they imitate similar systems operating on legitimate online trading forums such as eBay and Amazon Market. The strength of these systems lies not in the provision of completely accurate information, but rather in their capacity to create systems that self-regulate. While the fact remains that no individual piece of consumer feedback is necessarily true or verifiable, large volumes of comments are much more likely to be accurate. This is because once a critical mass of users begins providing feedback, the costs of attempting to manipulate that feedback by posting false messages increases. In other words, more and more false reviews become necessary in order to counter feedback that is genuinely provided. This means that as the size of a cryptomarket increases, and individual vendors attract larger volumes of user

DOI: 10.1057/9781137399052.0005

comments and ratings, the feedback system becomes more robust and the information that is provided is more likely to be accurate.

Support services and future research

In an indication of the increasing professionalisation and diversity of the online drugs trade, a range of cryptomarket support industries are beginning to emerge online. These offer different forms of specialist assistance for the budding dark net entrepreneur. Support services recently made available include: a web design company which, for the right amount of Bitcoins, will create a bespoke cryptomarket (CD 2014); a dark net marketing organisation, staffed by university-educated public relations experts who can "handle your 'advertising' while you focus on your sales" (DeepDotWeb 2014); and a new generation of search engine "patterned after Google" which will allow users to navigate the plethora of sites and products hidden on the dark net (Zetter 2014). How these new services develop and influence the future operations of cryptomarkets presents an intriguing area for future research.

Conclusion

This chapter has analysed how cryptomarkets operate from the perspectives of their users. Cryptomarkets are revealed as dynamic and complex commercial enterprises that manage the unique challenges associated with online, illicit and anonymous trading through the use of innovative website features and networked systems. These rely on the participation of users, including buyers and sellers, and affording both groups a central role in the ongoing development of the online drugs trade. While administrators are responsible for site construction, security, maintenance and other fundamental operations, it is users who ultimately determine the tone and the content of each site via the populating of vendor sub-pages and through providing consumer feedback. Cryptomarkets are therefore highly inclusive and representative of their users, who often display qualities that diverge significantly from those associated with people involved with the conventional trade in illicit drugs.

On cryptomarkets, many of the stereotypical qualities that are routinely (and sometimes erroneously) applied to distributors of illicit

DOI: 10.1057/9781137399052.0005

drugs – ruthlessness, capacity for violence, etc. – are far less relevant than is the case with offline drug distribution networks (see Chapter 3 for more detailed comparison and analysis of online vs. conventional drug distribution). In a highly competitive but physically disparate virtual environment, where violent exchange is effectively impossible, different skills and attributes are required for success. Instead of employing violent means, online drug dealers grow and maintain their market share by using a variety of business strategies, many of which are also found in the conventional retail sector. Indeed, it is remarkable how contemporary, legitimate marketing strategies are so readily adaptable to illicit drugs. This demonstrates that when facilitated by cryptomarkets, illicit drugs may be bought and sold much like other consumer commodities from the legitimate economy.

Note

1 In a further sign of the instability of the online illicit drugs trade, *TorMarket* recently closed down, taking with it all user funds waiting in escrow accounts. It is not yet known whether the loss of funds was due to an external attack or fraud carried out by the site's administrator.

DOI: 10.1057/9781137399052.0005

3

Conventional vs. Online Drug Distribution Networks

Abstract: *Chapter 3 presents a comparison between conventional drug distribution networks and those which are facilitated on the dark net. Various aspects of conventional drug distribution networks are analysed, including inefficiencies, product adulteration and systemic violence. Online distribution networks, by contrast, are associated with high levels of efficiency, improved product quality and minimal violence. The various relationships that form online between drug suppliers, retailers and consumers are also analysed.*

Martin, James. *Drugs On the Dark Net: How Cryptomarkets Are Transforming the Global Trade in Illicit Drugs.* Basingstoke: Palgrave Macmillan, 2014. DOI: 10.1057/9781137399052.0006.

Over the past two decades, researchers have made significant gains in conceptualising the ways in which illicit drug distribution networks operate and are structured. Gone are the days when the global drugs trade was believed to be dominated by pyramid-shaped criminal bureaucracies of the style portrayed in Francis Ford Coppola's 1972 classic, *The Godfather*. In fact, much contemporary research (Heber 2009, Malm and Bichler 2011, Bright and Delaney 2013) suggests quite the opposite: that illicit drug distribution is often carried out by decentralised groups, and that the involvement of rigidly hierarchical criminal organisations is relatively rare. Rather, criminal associations between individuals and groups adapt constantly to changing conditions, with relationships forming and dissolving according to emerging risks and opportunities. Even the dreaded narco 'cartels' of Central and South America have been revealed as far more fragmented (though no less deadly) than was once commonly thought (Kenney 2007, Benson and Decker 2010). From the dusty streets of Bogota to the urban ghettos of Europe, the idea of the monolithic 'evil empire' of organised crime appears increasingly inaccurate. Researchers are now documenting a mass of evolving and competing groups whose dynamism and ephemeral nature makes them particularly challenging subjects for research. This chapter explores the general characteristics associated with these illicit drug distribution groups before comparing them with new modes of distribution being facilitated online.

Social network analysis (SNA) is an increasingly popular tool amongst researchers seeking to map the various groups and individuals involved with illicit drug distribution. SNA conceptualises each participant in the distribution process as an individual node operating within a broader network. Each network necessarily includes both drug producers and consumers who are usually connected through an array of intermediary nodes, such as traffickers, wholesalers and street dealers. The networks themselves may be relatively small and simple, comprising only a few individual nodes. An example of this would be a small-time cannabis dealer who shares home-grown produce only with close friends and associates. Alternatively, networks may be large and complex; they may involve many thousands of individuals and loose syndicates which operate alongside more discrete organised crime groups such as gangs and mafias (Natarajan 2006, Malm and Bichler 2011, Ritter, Bright et al. 2012). Regardless of the size, complexity and transience of any drug distributing operation, the network model may be adapted to reflect the overall organisation and relationships between each of the participating nodes. Networks can reflect an almost limitless variety of configurations – from

DOI: 10.1057/97811373990520006

single-link supply chains, to pyramid-like hierarchies, decentralised and complex webs and any combination in between.

Limitations of social network analysis

The strength of SNA, as with any conceptual tool, is ultimately dependent upon the quantity and quality of primary data that are available. This points to one of the more significant problems currently limiting understanding of contemporary drug distribution: a lack of comprehensive and robust data. Unlike networks operating in the legitimate economy, illicit networks are shrouded in secrecy, and offenders understandably often go to great lengths to conceal the nature and extent of their involvement. While scholars have enjoyed some success in gathering ethnographic and other forms of primary data (see Ritter 2006), much of the information regarding illicit distribution networks comes from the variety of regional, national and transnational law enforcement agencies tasked with maintaining drug prohibition. This information is released in general reports, for example those produced annually by the United Nations Office on Drugs and Crime or the Australian Crime Commission, or as more specific intelligence in the form of police reports, courtroom testimonies, wire-taps and other forms of surveillance data (Malm and Bichler 2011, Calderoni 2012).

Relying on information produced by law enforcement agencies comes with its own problems. In many cases, detailed investigative intelligence remains confidential and is not released into the public domain (Edwards and Levi 2008). When this type of data are made available it may contain significant gaps, even when drawn from the most rigorous criminal investigations. This is due, at least in part, to the contrasting priorities of law enforcement and academia. When illegal enterprises are detected by law enforcement, the principal priorities for investigators are the targeting of 'main players' and gathering sufficient evidence for prosecution (Eck and Gersh 2000, Natarajan 2006). Information that is not immediately relevant to the prosecution, but has great potential value to criminologists and other scholars (for example, detailed network contours or the relational distribution of periphery nodes), is of a lesser priority and may therefore be neglected or excluded. Alternatively, investigators may completely miss the participation of important nodes and identify only partial sections of an illicit network (Xu and Chen 2008). Whatever the cause, incomplete data have the potential to distort understanding of the distribution process and produce erroneous impressions of network composition.

DOI: 10.1057/9781137399052.0006

Natarajan (2006), in her analysis of wire-tap data gathered as part of a large-scale investigation into heroin distribution in New York, provides an illustrative example of the problems that are associated with relying on intelligence provided by law enforcement. Amongst the 238 subjects who were placed under wire-tap surveillance, 35 were eventually charged by authorities who claimed that collectively the offenders represented a transnational drug trafficking organisation. The problem with this assertion was that while the offenders were found to be involved in drug distribution, they were not necessarily *organised* to do so in any concrete fashion. While the 35 offenders acted to affect a common purpose (i.e. the distribution and sale of heroin), and were demonstrably *associated*, this does not necessarily constitute their forming a discrete organisation. As Natarajan (2006) explains:

> It might be that the "organization" described in this paper had no real structural existence beyond that imposed on it by the actions of law enforcement... [instead] the "organization" might have been defined only by the resource limitations of a law enforcement operation. (Natarajan 2006: 189)

This example is significant in that it demonstrates how limited data, organisational bias and selective interpretation may compromise SNA of illicit distribution networks. If Natarajan's (2006) suggestion is correct, then police and prosecutors drew an artificial boundary around a set of related drug distribution nodes and simply labelled it an organisation. Presumably, if investigative resources had not been so limited, then more participating nodes would have been identified and subsequently incorporated into the 'organisation'. Clearly there are limitations with this kind of interpretation of law enforcement data. Determining the existence of a criminal groups or networks on the basis of operational expediency, rather than empirical fact, may be a practical necessity for law enforcement. However, it is certainly not reflective of good research practice and provides an important reminder of potential conflicting institutional imperatives within a shared research environment.

Characteristics of conventional illicit networks

Illicit networks, regardless of whether they are face-to-face or are facilitated online, are not created from the 'top down', but rather evolve

DOI: 10.1057/97811373990520006

organically in response to immediate pressures and conditions (Bright and Delaney 2013). As Calderoni (2012: 323) notes, "it is the market which shapes the criminal actors, not the other way round". This suggests that there is no standard organisational format for an illicit drug distribution network; rather each network adapts to the unique exigencies of its local environment. Despite this variability, a range of features that are common to many illicit drug distribution networks may still be determined. This is possible due to the presence of universal constraints which, to a greater or lesser extent, affect all illicit markets. These include a lack of trust between drug distributors, competition from other groups and individuals and threats posed by law enforcement (Anthony and Fries 2004, Bright and Delaney 2013).

Common constraints produce similar adaptive responses across various illicit distribution networks. Bright and Delaney (2013) suggest that a useful way of understanding the process of network adaptation is by drawing on the evolutionary principles that govern individual biology. In the biological sciences, similarities produced by shared environmental constraints (as opposed to genetic proximity) are determined cases of 'convergent evolution'. Convergent evolution explains how organisms with only distant genetic relations evolve similar features (e.g. sharp claws, spiky protrusions or camouflage) in response to external threats. In much the same way, common threats and selection pressures, particularly those posed by law enforcement and violent, intra-market competition, also shape networks operating across the criminal world, producing convergent formations across geographically and culturally disparate drug markets. The following section identifies the principal characteristics that are common amongst conventional drug distribution networks.

Network size and nodal redundancy

Conventional illicit drug distribution networks are often large, spanning long distances and traversing national borders. These networks comprise multiple distributing nodes, with each individual or group usually only controlling a limited section of the route of supply (Kenney 2007). This is partly the result of logistical necessity. Transnational drug distribution is complex and involves multiple stages of smuggling/trafficking, wholesaling and warehousing, as well as mid-level and street retailing.

DOI: 10.1057/97811373990520006

Distributing nodes operating at one point in the supply chain may lack the expertise, contacts or infrastructure necessary to participate effectively at other points in the network. For example, organised crime groups involved with international trafficking often have legitimate business interests and personal contacts or kinship ties in foreign locations (Kenney 2007, Calderoni 2012). These are specialist capacities that are particularly useful in facilitating the international sale and transportation of illicit drugs. Once drugs arrive in a foreign location, however, different capacities (e.g. knowledge of local conditions, political connections) are required in order to continue the distribution process. Smuggled goods may therefore be sold to local wholesalers, then on to other distributing nodes who are lower down in the chain of supply. Through this process, a single batch of illicit drugs may be exchanged between many different groups and individuals before finally being delivered into the hands of a consumer (Caulkins and Kleiman 2011).

In addition to network adaptations that are prompted by logistical pressures, conventional drug distribution networks tend to be lengthy and consist of large numbers of nodes for reasons related to security. Detection and arrest by law enforcement is an ever-present threat facing every participant in an illicit network. However, this threat is not equally distributed, with some roles and positions more exposed than others. Bouchard and Ouellet (2011) identify street or retail-level dealers as those running the greatest levels of risk within a drug distribution network. This is due to the fact that the work of street dealers necessarily renders them at least minimally visible to the broader public. This is necessary in order for dealers to meet new customers, supply existing ones and conduct everyday transactions. Unfortunately (at least, for drug dealers and their customers), this public profile also exposes them to the attentions of law enforcement, which targets low-level drug retailers through undercover buy/bust operations or large-scale raids on drug 'hotspots' where retailing activities are known to be concentrated (see Chapter 4 for a more detailed discussion of drug law enforcement tactics).

The risks associated with operating at a retail level are significant not only for street dealers, who can (and often do) find themselves charged and in police custody, but also for other distributing nodes who occupy adjacent positions in distribution network. Street dealers who are arrested have an incentive to cooperate with law enforcement and 'give up' their immediate contacts in order to have charges dropped or custodial sentences reduced. Alternatively, street dealers may unwittingly lead

DOI: 10.1057/97811373990520006

police surveillance to their suppliers or to other distributing nodes with whom they share direct contact. In either case, every node that is directly connected to a street dealer is exposed to an additional degree of risk. Researchers have identified that drug distributors can manage this risk by introducing additional intermediary nodes (Morselli, Giguère et al. 2007, Heber 2009, Bouchard and Ouellet 2011). These otherwise superfluous nodes act as buffers between highly exposed retail operations and other stages of distribution located further along in the network, such as wholesaling and mid-level supply.

Intermediary or 'buffer' nodes are not critical to the everyday, logistical functioning of an illicit network; their greatest value is realised not during uninterrupted operations, but when the network comes under assault from external parties, particularly law enforcement. When this occurs, buffer nodes absorb some of the damage that is done to the network through arrest and incarceration. This limits penetration of the more important parts of the network and provides targets for law enforcement that may be removed from the network without significantly disrupting its overall function. Buffer nodes may therefore be thought of as providing a reserve of 'nodal redundancy'. Nodal redundancy contributes significantly to the resilience of an illicit network, bolstering its capacity to weather the inevitable attrition which comes with operating in highly exposed and risky drug operations.

Network inefficiencies – price mark-ups and product adulteration

The resilience afforded by nodal redundancy does, however, come at a cost. As with any form of commercial enterprise, nodes that operate within an illicit distribution network must be compensated in some way for their participation. One way in which this compensation is achieved is by each node imposing a financial impost or 'mark-up' on an illicit good before it is passed on to a subsequent node. At every point of transaction within a supply chain, some form of price increase is likely to be imposed on the illicit drug which is then retained by each distributing node as profit. In principle, this process is no different from the price increases witnessed across legitimate supply chains, with the exception that there are relatively higher risks associated with illicit drug distribution (e.g. arrest, violence) which add a further premium to each price increase.

DOI: 10.1057/9781137399052.0006

While the total number of transactions and associated price increases varies between different drug markets and supply routes, Caulkins and Kleiman (2011) claim that there may be as many as ten transactions between the initial point of production and the end consumer. High numbers of transactions account for the often huge disparity between the initial 'farm gate' or 'factory gate' value of an illicit drug at its point of production and the final retail price paid by a consumer. According to Caulkins and Reuter (2010) these can vary by margins as high as 100:1.

The other manner by which nodes may be compensated for their involvement in the distribution process is to adulterate drugs before they are sold on. Adulterating or 'cutting' involves diluting drugs with cheaper substances so as to increase their overall volume. Through this process, distributing nodes artificially boost the quantity of drugs that are available for sale (either at the same or an incrementally higher price), thus providing another avenue whereby profit can be made. Product adulteration is a common practice across various illicit drug markets, particularly amongst synthetic and semi-synthetic drugs, and it accounts for why the purity of these goods typically decreases as they make their way through a distribution network (Ritter, Bright et al. 2012).

These two processes – incremental price increases and product adulteration – operate concurrently, simultaneously increasing the price and diluting the quality of illicit drugs as they make their way through a distribution network. Together they constitute the most significant inefficiencies inherent to conventional illicit distribution networks. The overall level of inefficiency is proportional to the size of the network; for every additional link included in the chain of supply there is a further opportunity for price increases and product adulteration.

Systemic violence

Undoubtedly, the most alarming aspect of conventional illicit distribution networks is their association with violence. Violence is systemically related to each stage of illicit drug distribution, from the initial point of production all the way through to the end consumer. It ranges from small-scale offences (e.g. minor assaults and intimidation between members of a drug-dealing gang), to nationally devastating conflicts, as may currently be witnessed in Mexico where drug-related conflict has claimed tens of thousands of lives over the past decade (Moreno 2014). Violence is endemic to illicit drug

DOI: 10.1057/97811373990520006

markets due to the vast profits, illegality and structural nature of drug manufacturing, retailing and supply. It is employed by drug manufacturers and distributors for various purposes, including: protecting production assets, personnel and commodities; excluding rival groups from trafficking routes and retailing 'turf'; dispute resolution and enforcing business contracts; maintaining internal group discipline; 'encouraging' compliance amongst corrupt politicians and law enforcement agents; and intimidating or killing outright opposing forces – whether they are law enforcement agents or other representatives of the criminal justice system, politicians, commentators or members of the general public. Extreme levels of violence can, however, be detrimental to productivity and profitability, and scholars (Ritter et al. 2002) note that lower levels of force are generally the norm amongst stable illicit drug markets.

Online distribution networks

Online drug distribution networks differ from conventional types in a number of significant ways. This is due to the different opportunities and constraints associated with operating illegal enterprises in a virtual as opposed to face-to-face environment. As discussed in the previous sections, conventional illicit networks are characterised by their decentralisation, complexity, varying degrees of nodal redundancy and association with systemic violence. These characteristics result from the need to counter or minimise external threats, particularly those posed by rival criminal organisations and law enforcement agencies. Online networks, by contrast, are distinguished by direct (or at least more direct) connections between drug producers and consumers, the participation of far fewer intermediary nodes and a higher overall level of network efficiency. This is made possible because the internet and associated anonymising technologies, particularly TOR encryption and cryptocurrencies (see Chapter 1), provide vital buffers between various distributing nodes and consumers. This dramatically alters the dynamics of network association and reduces the necessity for deterrence and competition premised on the use of force.

The most significant structural difference between online and conventional illicit distribution networks is the overall number of nodes that are required for the network to function effectively. Unlike conventional distribution networks, where a wide range of nodes specialise in different

DOI: 10.1057/97811373990520006

stages of distribution (e.g. trafficking, wholesaling), networks facilitated online are able to connect nodes and end consumers, in the absence of geographic proximity or interpersonal contact. This direct connection is facilitated by the cryptomarket itself which plays the critical role of broker. As with conventional brokers (Kenney 2007), cryptomarkets offers assurances of reliability and trust. This is achieved through various website innovations that track and reward responsible trading activity (see Chapter 2 for a more detailed discussion of consumer feedback and user tracking systems). Unlike conventional brokers, however, illicit sites are not limited by having to forge interpersonal relationships through friendships, kinship ties or other personal contacts. Instead 'trust' is represented through quantified metrics, such as the number of successful transactions carried out and publicly available feedback from consumers. The automation and user involvement associated with these processes mean that cryptomarkets are able to act as a kind of 'super broker', providing vast amounts of useful and transparent information about the trustworthiness of various users, and simultaneously connecting thousands of drug vendors with an even greater multitude of consumers.

There are three primary network formations which are facilitated via cryptomarkets. The nature and implications of these are described below.

Direct distribution: producer → consumer

The most radical online network formations are those that form directly between drug producers and consumers. As previously noted, direct exchange between producers and end consumers is generally not feasible in the context of conventional drug trading due to: 1) logistical barriers separating sites of production and consumption and 2) the risk of inadvertently selling illegal goods to a criminal informer or an undercover law enforcement operative. Neither of these challenges is insurmountable when trading online; complex logistical challenges are overcome through the use traditional postal services. Perhaps more importantly, encryption technologies and geographic separation insulate online retailers against threats posed by law enforcement, as well as by predatory criminal groups. Given that agencies such as the FBI publicly admit to buying drugs on cryptomarkets (FBI 2014), vendors are likely to assume that any of their customers could potentially be law enforcement

DOI: 10.1057/9781137399052.0006

agents operating undercover and consequently take whatever steps necessary to preserve their anonymity.

The direct relationships now forming between drug producers and consumers on cryptomarkets (see, for example DPPS 2013) have two major implications. Firstly, they represent a much more efficient method of distribution when compared to conventional, interpersonal drug networks. Direct links between producers and consumers bypass all the intermediary nodes comprising a conventional distribution network, effectively rendering wholesalers, traffickers and street retailers completely redundant. This allows drugs to be delivered without the need for additional financial imposts and also precludes the possibility of products being adulterated before they reach a consumer (although there is no guarantee that drugs will initially be produced or manufactured to a high standard). Direct distribution therefore allows products to be delivered more cheaply than through conventional means which results in greater savings and profit for producers and consumers, whilst also preserving their quality/purity.

Secondly, and most importantly in facilitating direct links between producers and consumers, cryptomarkets limit the potential for much of the systemic violence and other organised crime that is inherent to conventional illicit drug distribution networks. As online drug producers are able to operate anonymously there is no need to associate with organised crime groups for protection or to facilitate sales. Territorial street dealers are substituted in favour of anonymous letters arriving quietly in the post, thereby removing the potential for 'turf wars' between narco gangs and individual retailers. Risky interpersonal drug deals involving large quantities of drugs and cash are rendered obsolete, replaced in favour of smaller transactions between parties who never meet face-to-face (Christin 2013). Disputes may be resolved online by vendors with a vested interest in maintaining high levels of customer satisfaction.

For these reasons, direct distribution represents a much safer and more profitable form of illicit exchange for both drug producers and consumers. Further benefits also flow to members of the general public who are no longer exposed to the risk of death or injury as a result of being caught in the crossfire between rival drug gangs or predatory standover men. On the contrary, those with the most to lose from the formation of direct links between producers and consumers are members of criminal networks who use violence to control conventional drug distribution,

DOI: 10.1057/9781137399052.0006

and who currently profit the most from the illicit drugs trade (Kenney 2007, Calderoni 2012).

Semi-direct distribution: wholesaler → consumer

Unfortunately, direct distribution between producers and consumers is feasible only with certain kinds of illicit drugs, specifically those which are either grown organically (e.g. cannabis, hallucinogenic mushrooms) or manufactured synthetically (e.g. ecstasy, amphetamine). Semi-synthetic drugs, such as cocaine and heroin, maybe obtained only with the involvement of a much greater range of organised crime groups. This is because semi-synthetic drugs typically have long and complex supply chains. These involve cultivation and various stages of refinement in remote regions (e.g. coca in South America, opium poppy in Afghanistan or Southeast Asia) before goods are trafficked to consumer nations (Gibson, Degenhardt et al. 2003). Groups that are involved with these early stages of production (e.g. peasant farmers in the 'Golden Crescent' or 'Golden Triangle') are unlikely to have access to the technological infrastructure necessary to sell goods via a cryptomarket such as internet-enabled computers and secure postal systems. The earliest stage of distribution for these drugs to be realistically sold online is when they reach a wholesaler.

Wholesalers may sell drugs via a cryptomarket from either transit or destination countries. Those located in transit countries will be able to offer relatively cheaper products because they have not incurred the various overheads associated with international trafficking. By contrast, wholesalers in source countries will have relatively more expensive goods, but will also have a much greater chance of being able to deliver them successfully to a consumer. This is because packages sent within a source country are not subject to the same levels of inspection by customs and border protection agencies as those coming from foreign locations. Drug consignments sent from transit countries, particularly those with an association with drug production/trafficking, are much more likely to be intercepted by postal inspectors (see Chapter 4 for further discussion about vendors, postal smuggling and law enforcement).

Despite these limitations, semi-direct distribution still offers significant benefits to both online traders and members of the general public when compared to conventional modes of distribution. As is the case with

DOI: 10.1057/97811373990520006

the previous direct distribution model, wholesalers who sell to online customers bypass those distribution nodes involved with the latter stages of distribution, such as mid-level wholesaling and street retailing. This reduces the potential for systemic drug violence in destination countries, while also lessening the opportunities for product adulteration. Importantly, however, the involvement of supply-side organised crime groups (i.e. those who sell drugs to wholesalers) remains essentially unchanged. This means that the proliferation of cryptomarkets is unlikely to reduce the most serious forms of systemic drug crime, such as political corruption and violence, which currently plague drug production and trafficking hubs such as Mexico (Morris 2013).

Business to business: producer/wholesaler → retailer

The world's first cryptomarket-related arrest was carried out in Western Australia in early 2013 (Solon 2013). Interestingly, the offender was neither a producer nor end consumer, but rather a local dealer who purchased ecstasy and cocaine from overseas vendors before 'on-selling' to already established personal customers. Aldridge and Décary-Hétu (2014) identify this as a 'business to business' mode of online distribution. Their quantitative analysis of *Silk Road 1.0* indicates that between 31 and 45% of revenue generated on the site was associated with large volume sales which are likely to be for further retailing rather than personal use (Aldridge and Décary-Hétu 2014: 1). Conventional retailers are likely to be attracted to cryptomarkets because of the broad range of relatively cheap and high quality of drugs that are available online. These can be sourced on demand and without the need to associate with local organised crime groups who expect a percentage of the profits of whatever drugs they supply. Compared with other online network formations, the business to business model more closely resembles the conventional illicit drugs trade. However, significant benefits remain through the elimination of *some* conventional distributing nodes, thereby affording consumers and retailers advantages in terms of better prices and quality. More importantly, benefits are also likely flow through to the broader public as systemic crime and violence are reduced across the mid-level and the retail sections of drug distribution networks (Aldridge and Décary-Hétu 2014).

These three network formations represent the different means by which illicit drugs sold through a cryptomarket may reach a consumer.

DOI: 10.1057/9781137399052.0006

With the exception of the *Silk Road 1.0* study conducted by Aldridge and Décary-Hétu (2014), there is precious little research regarding which formations are the most prolific and what their implications might be. Given the potential benefits associated with the various modes of online distribution, this represents a worthy area for future research.

Conclusion

This chapter has analysed the structure and characteristics of both offline and online cryptomarket-facilitated distribution networks. Compared to the inefficiencies and violence associated with the conventional drugs trade, online networks present a preferable alternative. They offer significant benefits to drug traders in the form of safer methods of exchange and dispute resolution, greater profit margins for producers and cheaper and better quality products for consumers. Most significantly, direct and semi-direct distribution models have the potential to eliminate much of the organised crime and systemic violence associated with illicit drugs. Paradoxically, the growth of this new form of maligned cybercrime and illicit exchange may ultimately result in a net benefit to public safety.

The systemic advantages associated with online drug distribution suggest that cryptomarkets will continue to grow at the expense of interpersonal drug networks, assuming a greater proportion of the market. Just as legitimate online shopping has revolutionised the traditional retail sector, so too may the global trade in illicit drugs be set for a radical online transformation.

DOI: 10.1057/97811373990520006

4

Cryptomarkets and Law Enforcement

Abstract: *The final chapter examines online drug trading from the perspective of law enforcement. The various approaches associated with policing cryptomarkets are explored, including specialised undercover operations, postal interdiction, and domestic evidence gathering and prosecution. Online drug traders are presented as significantly more challenging targets for law enforcement agencies when compared to those who conduct illicit transactions in-person. Finally, the ideological relationship between cryptomarket users and law enforcement agencies is analysed.*

Martin, James. *Drugs On the Dark Net: How Cryptomarkets Are Transforming the Global Trade in Illicit Drugs.* Basingstoke: Palgrave Macmillan, 2014. DOI: 10.1057/9781137399052.0007.

The preceding chapters have explored cryptomarkets from a variety of conceptual and empirical perspectives, including those of both buyers and sellers seeking to trade illicit drugs online. This chapter shifts the focus analysis to a state perspective, with an emphasis on the conflict between law enforcement agencies and cryptomarkets, as well as the challenges associated with combating online drug distribution. Not surprisingly states, and law enforcement agencies in particular, are overwhelmingly hostile to cryptomarkets. This is due to the fact that these illicit websites operate beyond state control; publicly flout national and international laws; perpetuate (some of) the socially harmful effects of drug use and evade state-imposed taxes and tariffs that are levied on legitimate commercial goods and services. These and other factors suggest that from a state perspective, the various activities that are associated with cryptomarkets are perceived as subversive and criminal, as well as socially and economically harmful.

While typically slow to respond to threats emerging from the cyber-realm (Williams 2007, Thaxter 2010), in recent years states have singled out cryptomarkets as targets and stepped up efforts to combat their growing popularity amongst the drug taking public. There is a range of means by which states can combat cryptomarket-facilitated drug distribution. These include conducting specialised anti-cryptomarket cyber-policing operations. These can be used to gather evidence about users and administrators of cryptomarkets through the use of digital forensics, as well as through undercover infiltration of cryptomarket organisational structures (DPPS 2014, FBI 2014). Alternatively, states can indirectly target cryptomarkets by bolstering the conventional anti-drug capacities of law enforcement, for example, improving mail scanning procedures so as to intercept more drugs as they are sent through postal networks (AFP 2012). Finally, states may seek to undermine the infrastructure upon which online traders are dependent, such as the TOR network and Bitcoin or other cryptocurrencies, although this latter option is likely to be less attractive than it was in previous years due to the increasing utilisation of cryptocurrencies by non-criminal parties (including legitimate financial investors and currency speculators) (Levin, O'Brien et al. 2014).

Specialised anti-cryptomarket operations

The most significant victory for law enforcement in terms of direct attacks on cryptomarkets occurred in late 2013 when the US Federal

DOI: 10.1057/9781137399052.0007

Bureau of Investigation successfully infiltrated the leadership of the flagship site *Silk Road 1.0*. The outcomes of this lengthy, two and half year operation included the closure of the world's biggest online drug bazaar and the arrest of the alleged *Silk Road 1.0* creator and mastermind, Ross Ulbricht, formerly known only by the online moniker *Dread Pirate Roberts*. Intelligence gathered as part of the *Silk Road 1.0* investigation continues to facilitate the arrests of alleged drug vendors in the United States, Europe and Australia (NCA 2013, Cawrey 2014, FBI 2014), as the FBI and allied law enforcement agencies sift through seized databases and trace evidence left online. In the wake of these investigations, tens of millions of dollars' worth of Bitcoins have also been seized by state authorities, although claims made by the FBI that *Silk Road 1.0* turned over more than a billion dollars in illegal drug revenue (FBI 2014) are inaccurate and highly misleading.[1] Notwithstanding the exaggeration of the monetary value of illicit drugs that were traded through *Silk Road 1.0*, the FBI operation was a remarkable success and damaged online drug trading in ways far beyond the immediate handful of arrests and seizures.

At the time, the closure of *Silk Road 1.0* was hailed by law enforcement agencies and sections of the commentariat as proof that cryptomarket-facilitated drug dealing was no longer beyond the realm of state policing. Capitalising on the achievements of the FBI, law enforcement agencies across North America, Europe and Australia declared the beginning of the end for online drug distribution (NCA 2013, Cronshaw 2014, DEA 2014). These statements echoed the sentiments of the US prosecutors who indicted the alleged mastermind behind *Silk Road 1.0*:

> With his [Ulbricht's] arrest and our subsequent seizures of millions of dollars worth of Silk Road's Bitcoins, we have sent a clear message to him and everyone else running criminal enterprises on the dark web: we are determined and equipped to hold you to account.
>
> *US Attorney Preet Bharara cited in FBI (2014)*

To a certain extent, this and similar claims on the part of law enforcement representatives are accurate; the closure of *Silk Road 1.0* indeed demonstrated that cryptomarkets are vulnerable to concerted and well-resourced investigations. After years of virtually uninterrupted illicit trading, this realisation sent a shockwave through the online drug world and wrought immediate changes to cryptomarket activity that have yet to be fully resolved. Despite the fact that a near-identical clone cryptomarket, *Silk Road 2.0,* made its online debut barely a month after the

DOI: 10.1057/9781137399052.0007

closure of the original site (Greenberg 2013), neither this nor any other cryptomarket has yet established the same level of market dominance or attracted so great a proportion of online drug vendors and consumers in the one virtual space. Rather, drug vendors and consumers who patronised *Silk Road 1.0* and similar, smaller sites have been rocked by one disaster after another as a string of cryptomarkets have been either pre-emptively shut down due to security flaws (*Black Market Reloaded*, *Atlantis*); hacked and looted by external parties (*Silk Road 2.0;* possibly *TorMarket*); or closed with site administrators defrauding customers and vendors and absconding with funds waiting in escrow (*Sheep Marketplace; also* possibly *TorMarket*). The closure of *Silk Road 1.0*, therefore, represented the end of an era of unprecedented growth but also of relative stability in the cryptomarket landscape. It remains to be seen whether the decentralised instability that was catalysed by the *Silk Road 1.0* closure represents a temporary period of turbulent transition or a volatile, new norm.

Tackling the hydra – decentralisation and increased security

The state of flux that characterises this current era of cryptomarket activity presents a paradox for law enforcement – that is, the closure of *Silk Road 1.0* is likely to have made the policing of cryptomarkets more, rather less difficult. This is due partly to the fact that cryptomarket trading is significantly more decentralised now than it was when *Silk Road 1.0* was operating at its peak. Decentralisation is a direct consequence of the *Silk Road 1.0* closure, as the absence of this once dominant site left a surplus of unserviced supply and demand and created a vacuum which other cryptomarkets have since been striving to fill. The multitude of new sites which emerged in the wake of the *Silk Road 1.0* closure has been dubbed by media commentators as evidence of the so-called 'hydra effect' (Greenberg 2013, Ormsby 2013). This colourful term – referring to the dreaded mythical beast whose magical powers of regeneration allowed it to grow two heads wherever one had been cut off – is somewhat misplaced, given that many of the so-called *Silk Road 1.0* replacement sites, such as *Black Market Reloaded*, *Sheep Marketplace* and *Pandora,* were operating long before *Silk Road 1.0* was taken offline. However, despite the flawed timeline, the essential logic underpinning the hydra

DOI: 10.1057/9781137399052.0007

effect is sound; each cryptomarket closure represents an opportunity for new sites to establish themselves and capture an unclaimed proportion of illicit market share and profit. There can be little doubt that the closure of *Silk Road 1.0* has stimulated the formation of new cryptomarkets.

The principal dilemma facing state agencies tasked with combating the multitude of these emerging sites is where to target scarce investigative resources. As no new illicit market has yet assumed a clear position of market leadership or dominance, selecting which sites to prioritise for investigation is unavoidably speculative. Further complicating potential investigations is the short lifecycle of many cryptomarkets. As previously noted, many of the high-profile sites that rose to prominence in the wake of the *Silk Road 1.0* closure folded in a relatively short space of time without the active intervention of law enforcement. While this may be interpreted as a victory of sorts, in that law enforcement agencies have helped to create a dangerous and unstable environment for online drug traders, it also compounds difficulties for cyber investigators who require a minimum length of time in order to conduct and conclude complex investigations. If scarce law enforcement resources had been allocated towards investigating any of the ill-fated successors to *Silk Road 1.0*, then each pre-emptive and unanticipated closure represents a significant expenditure of taxpayer funds with little or no tangible return (i.e. no arrests or drug seizures).

Further complicating the work of law enforcement agencies are recent increases in cryptomarket security. According to Van Buskirk, Roxburgh et al. (2014) administrators are heeding the lessons of the *Silk Road 1.0* closure and are taking extra steps to fortify their sites against external penetration. In improving site security, administrators are being aided by members of the cryptomarket and hacker communities who are providing specialist advice about potential security flaws that could allow investigators access to encrypted communications and server locations (Bradbury 2013). Given widespread public knowledge about the crucial role that undercover operations played in gathering evidence against the leadership of *Silk Road 1.0*, administrators are also likely to be hyper-vigilant regarding overtures from unknown parties in an effort to minimise their exposure to covert law enforcement operations.

Naturally, none of these measures guarantee that existing and future sites will remain safe from cyber investigators. On the contrary, as cryptomarket trading recovers from the *Silk Road 1.0* closure and regains popularity amongst drug vendors and consumers, it seems inevitable that

DOI: 10.1057/97811373990520007

another site will eventually be taken down by law enforcement.[2] What extra security measures do indicate, however, is that these illicit sites are becoming more difficult for law enforcement agencies to compromise through direct attacks. This suggests that specialised anti-cryptomarket investigations will increase in complexity, requiring greater time and expertise to successfully conclude. This does not bode well for future operations, particularly when considering that it took the combined efforts of the world's most powerful and well-resourced law enforcement agencies more than two years to successfully close down *Silk Road 1.0*.

Indirect policing – challenges for customs and border protection agencies

In the struggle against cryptomarkets, customs and border protection agencies represent the state's first lines of defence. These organisations have traditionally played a central role in disrupting transnational drug distribution through the monitoring of sea and airports, land borders and crossings, and through conducting joint investigations with local, federal and international policing agencies. Of particular relevance to this study is the role of customs agencies in inspecting foreign postal deliveries. In the Global North, where the majority of cryptomarket activity is concentrated (Christin 2013), customs agencies work in partnership with both public and private postal organisations in order to detect drugs and other contraband that are sent through international mail networks. Postal inspections regimes are often expansive and rigorous, particularly as mail crosses international borders. The *Australian Customs and Border Protection Service*, for example, conduct an external examination of *every* item of incoming international mail – some 150 million letters and parcels per annum – with at least some form of detection technology (i.e. x-ray scanner or drug detection dog) (ACBPS 2013). Similarly, Canadian customs visually inspect all items of foreign post for any sign of illegal activity (CBSA 2014). As a result of these inspections, tens of thousands of incoming mail items containing illicit drugs are intercepted around the world each year (WCO 2013).

Even with comprehensive levels of mail scanning, a proportion of postal-ordered illicit drugs still arrive successfully at their final destinations. In the absence of further research, it is not possible to estimate how many drug consignments successfully run the gauntlet of postal

DOI: 10.1057/9781137399052.0007

interdiction. However, successful transnational smuggling facilitated by cryptomarkets is evidenced by both positive customer reviews and steadily growing numbers of vendors who are prepared to send drugs to foreign locations (Christin 2013, Van Buskirk, Roxburgh et al. 2014). With such a large volume of legitimate international post in circulation, locating individual drug consignments which are concealed with a high degree of sophistication is proving beyond the capacity of the cursory scanning procedures that are levied on all incoming foreign postal items. This poses a problem for customs and border control agencies which are hampered by limited resources with which to conduct further, more rigorous postal examinations. Detailed and invasive inspections, where postal items are scanned with multiple detection devices and are physically opened and inspected by customs or postal workers, are highly costly in terms of both time and resources. Due to the significant expenses and delays associated with these procedures, it is not feasible for customs and border control agencies to impose this additional degree of scrutiny on all incoming foreign mail.

Policing intelligence and risk profiling

Rather than relying solely on cursory examinations of all incoming post, customs and border protection agencies employ a variety of forms of policing intelligence. These assist in determining which postal items present the highest levels of risk and should be targeted for additional, more invasive examinations (ANAO 2011). Policing intelligence comes in a variety of forms, including specific alerts about suspected offenders; for example, a police informer may provide the names and addresses of suspected members of a drug importation ring. This information may then be used by customs agents to inspect any foreign mail that is destined for the identified suspects. Policing intelligence is also used to inform the creation of risk matrixes. Risk matrixes identify suspicious postal items according to a pre-determined set of criteria. If a letter or package meets a sufficient number of risk indicators or 'red flags', such as being excessively bulky, emitting an odour or arriving from a region associated with drug production (e.g. Columbia, the Netherlands), then a more invasive inspection is conducted (Steffen and Candelaria 2012). Depending upon the overall risk profile and the outcome of any initial inspection, an invasive, internal examination may also be undertaken

DOI: 10.1057/97811373990520007

where the presence of illicit drugs can finally be determined and any evidence collected.

Policing intelligence is highly valuable in that it provides customs agencies with an evidence-based repository of knowledge that may be used to inform the allocation of scarce drug detection resources. Local, national and international law enforcement agencies not only accumulate and maintain their own policing intelligence, but also share this information with other partnering agencies around the world (Collins, Huttunen et al. 2007, AFP 2012, WCO 2013). This allows law enforcement agencies access to the latest information regarding emerging international smuggling methods, as well as shifts in sources of supply and other relevant trafficking trends. In the era prior to the development of cryptomarkets, shared policing intelligence afforded customs agencies a significant, long-term strategic advantage over the drug distribution groups they were targeting. Unlike law enforcement agencies which could readily accumulate, analyse and disseminate anti-smuggling intelligence, conventional geographically disparate drug distribution groups lacked the capacity (and, if they were proximate competitors, the motivation) to readily communicate with one another. This impeded drug distributors from sharing their experiences and learning from the mistakes of their predecessors and contemporaries.

Naturally, a lack of shared intelligence amongst conventional drug distributors did not completely preclude their developing effective postal drug trafficking strategies. These continue to be pursued through a variety of means, including: the corruption of customs and postal officials (Anderson 2014); the 'scatter gun' approach, whereby large quantities of illicit drugs are sent in small volumes in the knowledge that a significant percentage will be intercepted and seized (Chalk 2011), and simple trial and error (Caulkins, Burnett et al. 2009). With such huge demand for illicit drugs, and extraordinary profits associated with trafficking, some level of postal drug trafficking appears destined to persist regardless of how risky, expensive or inefficient the processes involved. The central point, however, is that up until recently there existed a clear knowledge gap in favour of law enforcement. This allowed customs agencies to benefit from decades' worth of accumulated anti-trafficking intelligence and expertise; drug distributors, on the other hand, were forced to develop new smuggling strategies largely in isolation from one another and in the face of serious risks, including arrest, incarceration and the loss of intercepted goods.

DOI: 10.1057/97811373990052.0007

Intelligence sharing on cryptomarkets

The stark asymmetry that has long characterised the intelligence resources available to customs agencies and postal drug traffickers is now being rebalanced. In this new era of global, instantaneous and encrypted communications, online drug distributors have begun to develop their own, shared repository of knowledge regarding effective concealment and counter-interdiction techniques. This free and publicly available information is rapidly accumulating on cryptomarket forums, covering a comprehensive range of trafficking-related topics, including: generalised and beginner guides to drug smuggling ('How To Package Drugs Discretly [sic] – Guide for Vendors'; 'The Art of Smuggling'); the strengths and limitations of particular drug detection and concealment technologies ('Drug sniffing dogs – what they can and can't smell'); as well as advice for buyers and sellers who believe they may have come to the attention of law enforcement ('Delayed packet arrived this morning'; 'Shit! Did I fuck up?'). Importantly, notices and warnings are also uploaded regarding developments in inspections and customs regimes that are relevant to specific countries and regions ('Canada Post important changes!'; 'Shipping Cocaine/Heroin/Powders to Australia? Learn how! 85% – 95% Success!'). Combined with real-time customer feedback, information-sharing on cryptomarkets alerts online drug vendors and consumers to changes in postal interdiction strategies almost as soon as they are implemented.

Information that is hosted on cryptomarkets and associated forums is derived from a variety of sources, many of which are undoubtedly of dubious value and accuracy. Anecdotal accounts, uninformed speculation, as well as commentary that may be applicable in one region but not in others may encourage prospective drug distributors to take badly informed risks. Other sources, however, are likely to be much more useful. These include advice pages from highly experienced drug smugglers with demonstrated records of success,[3] as well as confidential documents that have been leaked from state agencies and private companies involved with postal delivery. Examples of the latter may be easily found, for example, in the security and shipping discussion forums on *Silk Road 2.0*, where users have posted copies of detailed reports from various law enforcement agencies, including the FBI and DEA, about postal profiling and risk matrixes. Several 'Ask Me Anything' discussion threads have also been hosted by people claiming to be former or current employees

DOI: 10.1057/9781137399052.0007

of postal companies. In these they invite questions about different stages of mail screening and provide specific information as to what kinds of postal items attract suspicion. Interestingly, lengthy excerpts from academic sources, for example Steffen and Candelaria (2012), have also been shared on cryptomarket forums, although how useful a contribution these make to the efforts of postal drug smugglers is not yet known.

The depth of trafficking-related information that is now available to cryptomarket vendors – as well as to anyone else seeking to send illicit goods through the post – has significant implications for the effectiveness of postal interdiction regimes. Intelligence shared on forums provides drug distributors with a detailed, readily accessible and easily searchable 'one stop shop' regarding the latest and most successful postal smuggling and counter-interdiction techniques. This regularly updated body of knowledge can be used to help drug distributors adopt 'best practice' smuggling methods with demonstrated records of success, as well as inform the development of new counter-interdiction techniques and strategies. Cryptomarket intelligence also allows drug distributors to quickly gauge emergent risks and changing threats posed by law enforcement. This information may then be used to determine whether drugs should be sent to particular regions and what refund policies should be in place for goods that may be intercepted (see Chapter 2 for discussion of refunds and terms and conditions). From a strategic perspective, this intelligence is steadily eroding the long-term knowledge advantage previously enjoyed by law enforcement. This suggests that customs and border control agencies face an uphill battle in combating postal drug distribution as smugglers increasingly communicate with and learn from one another, employ more sophisticated and effective concealment techniques and adapt more quickly to emerging threats from law enforcement.

Postal interception and the collection of evidence

The idiosyncrasies of online drug trading not only complicate the work of policing agencies as they attempt to intercept drugs in postal transit, but also cause difficulties with regard to other stages of domestic law enforcement, including investigations, evidence gathering and prosecution. Unlike conventional distribution networks, where consumers are required to meet retailers in-person in order to exchange goods and monies, online drug distribution networks are geographically disparate

DOI: 10.1057/9781137399052.0007

and operate under conditions of anonymity. Online retailers are therefore able to communicate with their customers and deliver products without any face-to-face interaction. This absence of direct physical contact precludes law enforcement employing conventional anti-drug tactics, such as buy-bust operations and raids on dealing 'hotspots'. The inability to apprehend online dealers and customers physically exchanging cash and illicit drugs represents an important lost opportunity for law enforcement whereby offenders could be: 1) witnessed committing an offence and 2) arrested whilst in possession of illicit drugs and proceeds of crime. In the absence of these simple, tactically efficient and productive operations, compiling sufficient evidence in order to justify laying criminal charges – let alone secure a conviction in court – is much more problematic.

Instead of apprehending drug retailers and consumers as they make an illicit exchange, local law enforcement agencies targeting online drug offenders face a limited range of investigative options, many of which are both relatively resource intensive and more complex to successfully prosecute. At present, real-time observation of financial exchanges carried out via cryptomarkets is not possible due to TOR and cryptocurrency encryption technologies which, under normal circumstances, appears to confound even the most sophisticated online surveillance techniques (Abbot 2010). For investigators, this places the onus on the collection of physical evidence after an offence has been committed. Intercepting postal orders or even making purchases directly from cryptomarket vendors are two avenues whereby law enforcement agents may gather physical evidence against online drug offenders. Whilst difficult to detect in transit, any consignment of illicit drugs that does make its way into the hands of law enforcement provides a potentially rich source of information regarding both the buyer and seller, as well the nature and origin of any drugs that have been seized.

Forensic chemical profiling, for example, can determine the geographic origins of cultivated and semi-cultivated drugs (e.g. cannabis, cocaine, heroin), while analysis of synthetic drugs such as ecstasy or methamphetamine may reveal the presence of precursor chemicals and associated manufacturing processes (Collins, Huttunen et al. 2007). This intelligence may then be used to help domestic and international policing agencies compare and match profiles of seized drugs and determine likely regions of production and trafficking routes. Physical (as opposed to chemical) profiling of seized mail is also likely to hold clues that may

DOI: 10.1057/97811373990520007

assist law enforcement in identifying drug distributors and consumers. Examining postage stamps, for example, will quickly reveal the geographic origins of mail orders, while analysis of packaging materials may assist with the identification of concealment methods (e.g. bleach decontamination, vacuum sealing). Also, it may be possible to trace seized packaging components (e.g. moisture barrier bags) to particular manufacturers, batches of production and even individual retailers.

Return addresses and other deliberately provided sender information written on seized envelopes/packages or on any internal documentation will almost certainly be false, having been provided purely to avoid arousing the suspicion of postal inspectors (even the most confident drug retailer is unlikely to risk recording their real address or name on a drug package). Addressee information, on the other hand, is much more likely to be accurate. Consumers may be tempted to provide false names in order to throw off detection by law enforcement, or to provide an avenue of deniability if the package is intercepted in transit. However, purchasing guides hosted on cryptomarket forums regularly advise consumers to supply a correct name and address. This is to ensure that mail is delivered as usual; letters addressed to names that are not registered to a postal address are commonly believed to arouse the suspicion of postal workers who are familiar with the usual names and addresses on their route.

> It may sound weird, but using your real name and your real address is the safest way [to receive drugs]. P.O. boxes can be dangerous and using a name that doesn't reside at the address is suspicious.
>
> *User post, Silk Road 2.0 forum [accessed 28/1/2014]*

> Never use fake names, computers check for that. And vary your addresses so if one of your letters gets caught they won't catch your other clients.
>
> *Vendor post – Agora forum [accessed 21/5/2014]*

Customers who are determined to withhold their real name but who still wish to supply a correctly matching name and address are advised to use someone else's details, for example, those of a previous tenant or an inattentive neighbour (whose post-box is accessible).

Postal deliveries and covert surveillance

If law enforcement agents successfully intercept a package containing illicit drugs and believe that the addressee information is correct, they

DOI: 10.1057/9781137399052.0007

may still wish to gather additional evidence before proceeding with an arrest. This is because investigators are likely to be wary of prematurely laying charges due to the difficulties associated with proving, beyond a reasonable doubt, that a suspect knew that illicit drugs were in their possession. In the absence of corroborating evidence that confirms that an illicit transaction has taken place, suspects who receive a drug package are relatively well placed to deny knowledge of any drugs delivered. Again, cryptomarket forums provide a vital source of information to online traders seeking to minimise risks, advising consumers how to construct legal defences and bolster claims of plausible deniability. Consumer guides outline a range of precautionary measures after making a purchase online, including: avoiding signing for any postal deliveries; leaving packages unopened for a minimum period of time and providing tips regarding how to respond to enquiries from law enforcement.

> For both newbs and seasoned buyers alike... strike "RETURN TO SENDER" and/or "DONOT WANT" through our name and place the package(s) by the front door, like here you would put anything going back or being returned... The more patience you show, the more you can wait – the better your chances go from zip to 99% of fucking them out of any conviction on you! I mean you don't know the senders address, you are not expecting anything via the mail. Shrug? Hell! You can't be responsible...
>
> *Vendor post – Pandora forum [accessed 21/5/2014]*

> Look, if merely having drugs sent to you is enough to get someone in trouble then I could put every person who has ever harmed me behind bars for life by just dropping some packages in the mail. But it is not that simple. As the law enforcement manual above states PROOF OF KNOWLEDGE OF THE CONTENTS BY THE RECEIVER IS ABSOLUTELY NECESSARY TO PROVE A CASE!...Not admitting to anything is the first rule of accepting drug packages safely.
>
> *Vendor post – Silk Road 2.0* forum [accessed 21/5/2014]

A non-cooperative suspect who is in possession of an unopened package containing illicit drugs does not represent a promising start on the road to a successful drug prosecution. To compensate for the relative paucity of evidence that may be derived from simply arresting a suspect who receives a drug delivery, investigators may seek to gain further evidence through the use of covert surveillance. Potentially valuable surveillance measures include installing hidden cameras inside a suspect's residence so as to film them opening packages and handling the illicit drugs inside. Alternatively, tracking software could be manually installed on a suspect's computer,

DOI: 10.1057/9781137399052.0007

allowing incriminating communications and transactions to be recorded. If the targeted suspect is indeed guilty, these additional measures would provide compelling evidence and greatly assist in securing a conviction.

Despite the possibility of law enforcement employing these kinds of additional surveillance measures, there are significant limitations that preclude them from being utilised on wide scale. Firstly, surveillance operations are highly costly in terms of both manpower and technological resources (Harfield and Harfield 2008). Justifying the expenses associated with surveillance operations is likely to be difficult in the case of cryptomarket-facilitated drug deliveries. This is due to the fact that most deliveries contain only small quantities of illicit drugs, usually valued at less than $200 USD (Christin 2013). Small quantities of illicit drugs mean that even if a conviction is secured against an offender, it is likely to be for a minor possession rather than a more serious commercial distribution or trafficking charge.

Secondly, surveillance operations which require covert entry into suspect households are highly invasive. They represent a serious violation of an individual's rights to privacy and, in many jurisdictions, are only permissible under judicial oversight and when deemed proportionate to the seriousness of the crime under investigation (Harfield and Harfield 2008). Again, this would be difficult to justify in cases regarding small quantities of illicit drugs where broader threats to public safety are minimal. The bureaucracy associated with gaining the authorisation necessary to install covert surveillance inside a suspect's residence is likely to act as a further disincentive to law enforcement, particularly when these resources may be used to target street-based drug dealing without judicial approval.

Finally, unlike conventional drug investigations, where arrested suspects may be 'leveraged' to provide intelligence and evidence against suppliers and other co-offenders, arrests resulting from cryptomarket-facilitated drug deliveries cannot be followed further up the chain of supply. This is because at no stage do online consumers learn the real identities or physical locations of those from whom they purchase illicit drugs. Rather, consumers have access only to information which is provided on the vendor's seller page (e.g. the price of illicit goods, locations to which they may be sent). This means that any arrest of a cryptomarket consumer represents a dead end in terms of subsequent investigation. This is a significant limitation that further undermines the value of operations targeting the postal delivery stage of online drug distribution.

DOI: 10.1057/9781137399052.0007

Crypto-libertarians or cybercriminals? The battle for public legitimacy

The previous sections have analysed some of the main tactical and strategic difficulties facing law enforcement agencies in their fight against cryptomarkets. This final section explores the broader ideological and propaganda dimensions associated with this conflict. Given the illegality and the purported harms associated with these illicit online markets, a degree of hostility from the state was inevitable from the moment that they were launched. However, the current level of animosity between cryptomarket traders and law enforcement agencies is also one that actors on both sides have encouraged. Unlike proto-cryptomarkets such as *Farmer's Market*, which for over half a decade carried out a discrete, small-scale, illicit online trade (Heintz 2012), newer sites, particularly *Silk Road 1.0*, overtly challenged the power of the state. In late 2013, emboldened by over two years of largely uninterrupted growth, the administrator of *Silk Road 1.0*, *Dread Pirate Roberts*, publicly declared that the War on Drugs was over and that "the guys with the bongs have won" (Greenberg 2013). These provocative sentiments were expressed in a ten-page interview with *Forbes* magazine – better known for its annual world's richest list than interviews with international drug lords – where *Dread Pirate Roberts* outlined his ambition for a global crypto-anarchist revolution:

> We've won the State's War on Drugs because of Bitcoin, and this is just the beginning... The people now can control the flow and distribution of information, and the flow of money. Sector by sector the state is being cut out of the equation and power is being returned to the individual. I don't think anyone can comprehend the magnitude of the revolution we are in... It will be looked back on as an epoch in the evolution of mankind.
>
> *Dread Pirate Roberts, cited in Greenberg (2013)*

Given that the closure of *Silk Road 1.0* and the arrest of *Dread Pirate Roberts* occurred less than two months after the publication of this interview, it is tempting to interpret this statement as little more than badly timed and needlessly antagonistic rhetorical hubris. However, the sentiments expressed by *Dread Pirate Roberts* are also characteristic of a libertarian political philosophy regularly espoused by other cryptomarkets administrators (Ormsby 2013) (see Chapter 1 for further discussion of relevant political philosophies). Libertarianism is also a popular and often passionately supported topic on various cryptomarket forums, where

DOI: 10.1057/9781137399052.0007

'true believers' advocate online illicit trading as a less violent alternative to conventional drug retailing. Consider the following message from a *Silk Road 2.0* user addressed to law enforcement agencies suspected to be monitoring the site:

> Dearest law enforcement...
>
> Silk Road is not perfect... but this community has done something special. It has put the paper bag on drugs. The [silk] road keeps your streets a little cleaner, with fewer dealers polluting streets. The [silk] road reduces violence, it removes much of dangerous criminal element of drugs which make them a problem.
>
> Surely we can agree that targeting a group of online drug activists with a penchant for getting high is not worth the time of law enforcement agents such as yourselves. You are losing a drug war on the streets, people are dying as cartels spread their influence and gang violence endures.
>
> So why bother? Why bother devoting yourself to the eradication of this and other deep web communities? The [silk] road is the lesser evil, we all just wish you'd leave it be. There are good things you could be doing out there, policing the streets and preventing violence.
>
> *User post – Silk Road 2.0 forum [accessed 24/5/2014]*

Naturally, law enforcement representatives tend to reject the notion that those involved with the online drug trade are motivated by an aversion to violence, or by political rather than economic imperatives (although none of these motivations are necessarily mutually exclusive). Instead, they seek to portray cryptomarket administrators and vendors as ruthless villains focused solely upon the exploitation of a vulnerable and victimised public:

> The website was used by drug dealers to put illicit drugs into our communities and literally at our doorsteps nationwide. 200,000 people die annually from drug abuse throughout the world, and our investigators worked tirelessly to bring to justice a facilitator who made every effort to hide behind highly encrypted technology... Ulbricht's goals were to make millions from drug use and money laundering while protecting the world's criminals from law enforcement. Our goal is to shut these people down and protect our children and [the] DEA will continue to be relentless in this effort.
>
> *DEA Special Agent Crowell cited in FBI (2013)*

The views expressed by the DEA are consistent with other statements regarding cryptomarkets which have been made by law enforcement

DOI: 10.1057/97811373990520007

representatives from around the world (see, for example, DEA 2014, DPPS 2014, FBI 2014)). Together they represent an attempt to foster a public image of online drug traders as self-interested criminals who are highly dangerous (linked to the deaths of hundreds of thousands of drug users, targeting 'our children', etc.), and also cowardly (hiding behind encrypted technology).

While many are likely to simply accept these perspectives as claims to fact, there are also important propaganda dimensions to the negative characterisation of online drug offenders. Just as online drug traders have a self interest in legitimising their activities under the guise of political expression, so too do law enforcement agencies have an incentive to demonise their targets and inflate the public value of their own investigations. Framing the activities of cryptomarket traders as profit-driven, criminal exploitation is essential for law enforcement agencies that rely on public and political support in order to fund the vast apparatus of prohibition. With the financial costs of enforcement focused anti-drug policies estimated to cost taxpayers approximately $40 billion USD each year in the United States alone (Miron and Waldock 2010), it is critical that cryptomarkets (and, by extension, the drug distributors and consumers who use them) be portrayed as serious, unmitigated threats to society. In addition to justifying tens of billions of dollars spent on law enforcement budgets, an appropriately alarmed and outraged public is also necessary in order to advance organisational prestige, facilitate individual careers and internal promotion and justify the expansion of coercive state powers and surveillance (Baum 1996, Payan 2006).

The contrasting views of cryptomarkets as either non-violent sites of commercial exchange and political expression or centres of a new form of malign cyber-criminality represent two ends of a spectrum of public perception. Regardless of whether either (or neither) of these perspectives is accurate, their mutual coexistence creates the unusual state of affairs whereby both sides of the conflict claim to be acting in the public interest. This clash of ideas represents more than an intriguing backdrop to the tactical and strategic struggles between law enforcement and online drug distributors; rather, it is an essential part of the conflict. In claiming the moral high ground and portraying the state as guilty of authoritarian overreach, users of cryptomarkets are continuing a line of argument against the War on Drugs and in favour of harm minimisation.

At present mainstream public and political opinion appears to be on the side of law enforcement. However, there is no guarantee that this will

DOI: 10.1057/97811373990520007

remain the case indefinitely. After four decades of enforcement-led global prohibition, there is tentative evidence to suggest that tough anti-drug rhetoric may be failing to 'cut through' to a (drug) war-weary public and that hard-line policing and penal policies are losing some of their public appeal (Erceg-Hurn 2008, Kang, Cappella et al. 2009, Magura 2012). A number of countries in South America and Europe are either reducing or suspending entirely previously onerous drug laws (Ferreri-Hanberry 2013, Greenwald 2013). Even in the United States, the ideological home of the War on Drugs, public attitudes towards illicit drugs are softening, with state and federal legislatures reducing mandatory drug-related sentences (Subramanian and Moreno 2014), expanding the use of drugs for scientific or 'medicinal' purposes (Masten and Guenzburger 2014), and, in the states of Colorado and Washington, legalising the recreational use of marijuana (for a contrasting view see Alexander (2012).

How changing public attitudes towards illicit drugs will affect the policing of online drug markets in the long-term remains to be seen. What is increasingly apparent, however, is that unrestricted support for prohibition – let alone aggressive anti-drug law enforcement – can no longer be taken for granted. The potential of wavering public support for enforcement-led prohibition adds extra pressure on law enforcement agencies to maximise their rhetorical and ideological attacks on cryptomarkets, and also to implicate them with violence whenever possible. There is much at stake. The battle for public legitimacy will ultimately determine the fate of both cryptomarkets and prohibition agencies.

Conclusion

This chapter has explored the relationship between cryptomarkets and the state, and with law enforcement agencies in particular. From a state perspective, it is clear that online drug trading presents a much more complex range of tactical, strategic and ideological challenges when compared with conventional, in-person forms of illegal exchange. Online offenders are protected by highly powerful yet freely available encryption technologies; they interact anonymously and maintain geographic separation, which significantly complicates the critical task of collecting evidence. Cryptomarket users also readily communicate with one another and are developing their own counter-interdiction strategies and intelligence. This enables them to respond and adapt quickly to new threats

DOI: 10.1057/9781137399052.0007

posed by law enforcement. Because of these difficulties, law enforcement agencies will be forced to develop new approaches if they intend to successfully combat cryptomarket-facilitated drug distribution.

Investigators may well be determined to bring users and operators of cryptomarkets to justice, but whether they are presently equipped to do so long-term and on a sustainable basis remains very much in doubt. The resources available to even the biggest law enforcement agencies are finite and any efforts to strengthen specific anti-cryptomarket capacities will draw upon limited, specialist expertise – expertise that could arguably be used more effectively in targeting higher-priority crimes involving higher levels of violence or other more serious threats to public safety (e.g. state-sponsored cybercrime, cyber-terrorism).

The closure of *Silk Road 1.0* currently represents a high-water mark in the fight against online drug distribution. Unfortunately for law enforcement agencies, repeating this achievement against newer cryptomarkets is likely to be prohibitively costly, complex and time-consuming. Without a radical breakthrough in defeating TOR encryption or cryptocurrency technologies, cryptomarkets will likely continue on current trends towards further growth and diversification. In this new digital front of the War on Drugs, it looks as though the forces of prohibition are headed towards defeat.

Notes

1 The $1.2 billion USD figure quoted by the FBI was calculated according to the total number of Bitcoins traded through the site as valued at the time that the website was shut down (approx. $126 USD). This valuation is significantly higher than the rate at which Bitcoins were valued for the majority of the time *Silk Road 1.0* was in operation (Ormsby 2013).

2 In February 2014, Dutch police successfully infiltrated and closed down *Utopia*, despite the site having been in operation for only one week. According to a statement by Dutch prosecutors (DNP 2014), the arrested suspects were formerly associated with the popular cryptomarket *Black Market Reloaded* which was taken offline in 2013 due to security flaws (Bradbury 2013).

3 As noted in Chapter 1, when posting messages on cryptomarket forums, supplementary information is often provided regarding user histories, including the number of successful transactions that have been conducted.

DOI: 10.1057/9781137399052.0007

Conclusion and Future Directions

Abstract: *The final chapter offers concluding comments and observations on the present state of the online illicit drugs trade. Cryptomarkets are discussed as entering a new, 'post Silk Road' phase of activity characterised by increased competition, diversity and innovation. The question of whether the proliferation of cryptomarkets represents a positive or negative development ultimately depends on one's perspective.*

Martin, James. *Drugs On the Dark Net: How Cryptomarkets Are Transforming the Global Trade in Illicit Drugs.* Basingstoke: Palgrave Macmillan, 2014. DOI: 10.1057/9781137399052.0008.

DOI: 10.1057/9781137399052.0008

Drugs on the dark net appear to be here to stay. The various setbacks that have at times beset the online illicit trade – arrests, scams, the loss of funds and property – have each been followed by processes of recovery and reconsolidation. Individual cryptomarkets have shut down, and administrators and vendors imprisoned, yet the broader dark net community continues to adapt and thrive. It is evident that the closure of *Silk Road 1.0* was not the 'knockout' blow that some expected and indeed hoped it would be. On the contrary, this event may be interpreted as an act of creative destruction, an important catalyst for the diversity and renewed competition witnessed amongst the contemporary online drugs trade.

Cryptomarkets have now moved beyond *Silk Road 1.0* in to a new, more dynamic phase of activity. This is characterised by increasing decentralisation, competition and innovation. The current generation of administrators are creating novel website features, security services and marketing strategies in an effort to better connect with customers and stand out amidst an increasingly crowded online marketplace. In a further sign of convergence with businesses in the legitimate economy, a budding support services industry is emerging, offering professional assistance with web design, public relations and search optimisation. Amongst cryptomarket users, there appears to be more caution, cynicism, as well as less interest in, and enthusiasm for the ideological crusade launched by *Dread Pirate Roberts*. Utopian hubris is giving way to a more calculated and business-minded sense of defiance. Wearied by attacks from law enforcement, scammers, and inter-site migration, once idealistic consumers are being transformed into less sentimental veterans of the online drugs war.

Whether the ongoing success of cryptomarket trading ultimately represents a positive or negative development depends on one's perspective. For online consumers, producers and retailers, there are significant benefits. Cryptomarkets offer an alternative to the inefficiencies and violence inherent to the conventional drugs trade. Illicit goods may be sourced more cheaply, safely and, paradoxically, with greater levels of accountability when purchased anonymously online. Advantages also flow through to the general public in the form of less organised crime and violence as drug supply networks are reduced in size, or are replaced entirely by direct producer-consumer modes of distribution.

From the perspective of law enforcement agencies, the rise of online drug dealing is more ambivalent. On the one hand, cryptomarkets

DOI: 10.1057/97811373990520008

represent formidable enemies; they facilitate law-breaking, operate in open defiance of prohibition, and are extraordinarily difficult and resource intensive to investigate. On the other, they have the potential to reduce many of the systemic harms associated with the illicit drugs trade. These contrasting implications present a dilemma for law enforcement agencies. If they divert scare resources towards cryptomarkets, they risk forcing drug trading back into conventional networks at greater risk to public safety.

Understanding the various processes affecting cryptomarkets is critically important. If present trends continue, cryptomarkets will diversify further, increasing in popularity and assuming a greater proportion of the overall drugs market. In the long-term, these changes have the potential to radically transform the global illicit drugs trade, affecting producers, distributors, consumers, as well as law enforcement agencies and the general public. Precisely how these changes manifest, and what new, unanticipated challenges emerge are certain to constitute important and fascinating issues for future research.

DOI: 10.1057/97811373990052.0008

Bibliography

Abbot, R. (2010). "An Onion a Day Keeps the NSA Away." *Journal of Internet Law* **13**(11): 22–28.

Ablon, L., et al. (2014). *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar*, Rand Corporation.

ACBPS (2013). Australian Customs and Border Protection Service Annual Report 2012–2013, A. C. a. B. P. Service.

AFP (2012). *Drug Importers Targeted in Nationwide Parcel Post Blitz*. Canberra, Australia.

Aldridge, J. and D. Décary-Hétu (2014). "Not an 'Ebay for Drugs': The Cryptomarket 'Silk Road' as a Paradigm Shifting Criminal Innovation." *Available at SSRN*.

Alexander, M. (2012). *The New Jim Crow: Mass Incarceration in the Age of Colorblindness*, New York, The New Press.

ANAO (2011). *Risk Management in the Processing of Sea and Air Cargo Imports*.

Anderson, E. (2014). Edmond Postal Worker Accused of Trafficking Drugs. *News9.com*.

Anthony, R. and A. Fries (2004). "Empirical Modelling of Narcotics Trafficking from Farm Gate to Street." *Bull Narc*: 1–48.

Ball, J., et al. (2013). "NSA and GCHQ Target Tor Network That Protects Anonymity of Web Users." *The Guardian*, Guardian News and Media Limited.

Barratt, M. J. (2012). "Silk Road: eBay for Drugs." *Addiction* **107**(3): 683–683.

Barratt, M. J., et al. (2013). "Use of Silk Road, The Online Drug Marketplace, in the UK, Australia and the USA." *Addiction*.

DOI: 10.1057/97811373990520009

Barratt, M. J., et al. (2013). "Internet Content Regulation, Public Drug Websites and the Growth in Hidden Internet Services." *Drugs: Education, Prevention, and Policy* **20**(3): 195–202.

Baum, D. (1996). *Smoke and Mirrors: The War on Drugs and the Politics of Failure*. Boston, Little, Brown and Company.

Benson, J. S. and S. H. Decker (2010). "The Organizational Structure of International Drug Smuggling." *Journal of Criminal Justice* **38**(2): 130–138.

Bouchard, M. and F. Ouellet (2011). "Is Small Beautiful? The Link between Risks and Size in Illegal Drug Markets." *Global Crime* **12**(1): 70–86.

Bradbury, D. (2013). "Black Market Reloaded Back Online Following Source Code Publication Error." *CoinDesk: The Voice of Digital Currency*.

Bradbury, D. (2014). "Unveiling the Dark Web." *Network Security* **2014**(4): 14–17.

Brands, H. (2010). *Crime, Violence, and the Crisis in Guatemala: A Case Study in the Erosion of the State*, Strategic Studies Institute.

Brenner, S. (2010). *Cybercrime: Criminal Threats from Cyberspace*. Santa Barbara, California, Praeger.

Bright, D. A. and J. J. Delaney (2013). "Evolution of a Drug Trafficking Network: Mapping Changes in Network Structure and Function across Time." *Global Crime* **14**(2–3): 238–260.

Burris, S., et al. (2005). "Nodal Governance." *Austl. J. Leg. Phil.* **30**: 30.

Calderoni, F. (2012). "The Structure of Drug Trafficking Mafias: The 'Ndrangheta' and Cocaine." *Crime, Law and Social Change* **58**(3): 321–349.

Caulkins, J. P., et al. (2009). "How Illegal Drugs Enter an Island Country: Insights from Interviews with Incarcerated Smugglers." *Global Crime* **10**(1–2): 66–93.

Caulkins, J. P. and M. A. Kleiman (2011). "Drugs and Crime." *The Oxford Handbook of Crime and Criminal Justice*: 275.

Caulkins, J. P. and P. Reuter (2010). "How Drug Enforcement Affects Drug Prices." *Crime and Justice* **39**(1): 213–271.

Cawrey, D. (2014). "Australia May Extradite Alleged Silk Road Moderator to US." *CoinDesk*.

CBSA (2014). "Postal Program – Importing by Mail." Retrieved 23/5/2014, from http://www.cbsa-asfc.gc.ca/import/postal-postale/menu-eng.html.

DOI: 10.1057/97811373990520009

CD (2014). "Crypt Design: Design Services for the Dark Net." Retrieved 31/5/2014, 2014, from http://cryptdesign.com/.

Chalk, P. (2011). *The Latin American Drug Trade: Scope, Dimensions, Impact, and Response*, Rand Corporation.

Chen, J. and S. Dibb (2010). "Consumer Trust in the Online Retail Context: Exploring the Antecedents and Consequences." *Psychology & Marketing* **27**(4): 323–346.

Christin, N. (2013). *Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace*. Proceedings of the 22nd international conference on World Wide Web, International World Wide Web Conferences Steering Committee.

Collins, M., et al. (2007). "Illicit Drug Profiling: The Australian Experience." *Australian Journal of Forensic Sciences* **39**(1): 25–32.

Cronshaw, D. (2014). "Police Warnings over Buying Drugs, Fake IDs on 'Dark Net'." *Newcastle Herald*, Fairfax.

Curran, G. and M. Gibson (2013). "WikiLeaks, Anarchism and Technologies of Dissent." *Antipode* **45**(2): 294–314.

DEA (2014). Manhattan U.S. Attorney Announces Charges against Bitcoin Exchangers, Including CEO of Bitcoin Exchange Company, for Scheme to Sell and Launder over $1 Million in Bitcoins Related to Silk Road Drug Trafficking. U. S. D. E. Agency.

DeepDotWeb (2014). "Darknet Marketing Services" Is the New Emerging Market? *DeepDotWeb*.

DeepDotWeb (2014). Interview with "Cannabis Road" Lead Developer. *DeepDotWeb*.

DeepDotWeb (2014). Interview with Outlaw Market Admin. *DeepDotWeb*.

DeepDotWeb (2014). "Updated: List of Hidden Marketplaces (Tor & I2P)." Retrieved 30/5/2014.

Deutsch, K. (2013). DEA Probes Silk Road, Suspected Online Hub for Illegal Drugs. *Newsday*.

Dingledine, R., et al. (2004). Tor: The Second-Generation Onion Router, DTIC Document.

DPPS (2013). XTC Express Sidetracked, Dutch Public Prosecution Service.

DPPS (2014). Undercover Investigation into Illegal Marketplaces on the Internet, Dutch Public Prosecution Service.

Eck, J. E. and J. S. Gersh (2000). "Drug Trafficking as a Cottage Industry." *Crime Prevention Studies* **11**: 241–272.

DOI: 10.1057/9781137399052.0009

Edwards, A. and M. Levi (2008). "Researching the Organization of Serious Crimes." *Criminology and Criminal Justice* **8**(4): 363–388.

Erceg-Hurn, D. M. (2008). "Drugs, Money, and Graphic Ads: A Critical Review of the Montana Meth Project." *Prevention Science* **9**(4): 256–263.

Falconer, J. (2012). Mail-Order Drugs, Hitmen & Child Porn: A Journey into the Dark Corners of the Deep Web. *The Next Web*.

FBI (2013). Manhattan U.S. Attorney Announces Seizure of Additional $28 Million Worth of Bitcoins Belonging to Ross William Ulbricht, Alleged Owner and Operator of "Silk Road." Website US Federal Bureau of Investigation.

FBI (2014). Manhattan U.S. Attorney Announces the Indictment of Ross Ulbricht, the Creator and Owner of the Silk Road Website. New York, Federal Bureau of Investigation.

Ferreri-Hanberry (2013). "Ecuador Latest in Latin America to Decriminalize Drugs." *The Libertarian*.

Flitter, E. (2013). "FBI Shuts Alleged Online Drug Marketplace, Silk Road." *Reuters*, Thomson Reuters.

Foxton, W. (2013). "Crisis on the Silk Road: If You Can't Trust Britain's Biggest Online Drug Dealer, Who Can You Trust?" *The Telegraph*, Telegraph Media Group.

Gibson, A., et al. (2003). *Global and Australian Heroin Markets*, University of New South Wales, National Drug and Alcohol Research Centre.

Greenberg, A. (2013). "Meet The Dread Pirate Roberts, The Man Behind Booming Black Market Drug Website Silk Road." Retrieved 9/2, 2014, from http://www.forbes.com/sites/andygreenberg/2013/08/14/meet-the-dread-pirate-roberts-the-man-behind-booming-black-market-drug-website-silk-road/.

Greenberg, A. (2013). "New Silk Road Drug Market Backed Up To '500 Locations in 17 Countries' To Resist Another Takedown." *Forbes*.

Greenberg, A. (2013). "Silk Road Competitor Shuts Down and Another Plans to Go Offline After Claimed $6 Million Theft." *Forbes*.

Greenwald, G. (2013). "Drug Decriminalization in Portugal: Lessons for Creating Fair and Successful Drug Policies." *Gene*.

Grinberg, R. (2012). "Bitcoin: An Innovative Alternative Digital Currency."

Harfield, C. and K. Harfield (2008). *Covert Investigation*. Oxford, Oxford University Press.

DOI: 10.1057/97811373990520009

Heber, A. (2009). "The Networks of Drug Offenders." *Trends in Organized Crime* **12**(1): 1–20.
Hein, W., et al. (2010). "Conceptual Models for Global Health Governance." *Temple University Legal Studies Research Paper* (2010–20).
Heintz, L. (2012). "Here's The Indictment That Blew the Lid on the EBay of Drug Trafficking This Week." *Motherboard*, Vice Media Inc.
Hodson, H. (2013). "Silk Road Bust Hints at FBI's New Cybercrime Powers." *New Scientist* **220**(2938): 22.
Holt, T. (2013). *Crime On-Line: Correlates, Causes, and Context*. Durham, North Carolina, Carolina Academic Press.
Hout, M. C. and T. Bingham (2013). "'Silk Road', The Virtual Drug Marketplace: A Single Case Study of User Experiences." *International Journal of Drug Policy* **24**(5): 385–391.
Jewkes, Y., et al. (2010). "Introduction: The Internet, Cybercrime and the Challenges of the Twenty-First Century." *Handbook of Internet Crime.* Devon, Willan Publishing, 1–8.
Jivanda, T. (2014). "Teenager Patrick McMullen Who Died while on Skype Had Bought Drugs from Silk Road." *The Independent*.
Kang, Y., et al. (2009). "The Effect of Marijuana Scenes in Anti-Marijuana Public Service Announcements on Adolescents' Evaluation of Ad Effectiveness." *Health Communication* **24**(6): 483–493.
Karlstrøm, H. (2014). "Do Libertarians Dream of Electric Coins? The Material Embeddedness of Bitcoin." *Distinktion: Scandinavian Journal of Social Theory* (ahead-of-print): 1–14.
Kenney, M. (2007). "The Architecture of Drug Trafficking: Network Forms of Organisation in the Colombian Cocaine Trade." *Global Crime* **8**(3): 233–259.
Kerr, D. (2013). "Silk Road Drug Busts Multiply, Eight New People Arrested." *CNET*, CBS Interactive.
Leger, D. (2014). "How FBI Brought Down Cyber-Underworld Site Silk Road." *USA Today*, Gannett Satellite Information Network.
Levin, R. B., et al. (2014). "Dread Pirate Roberts, Byzantine Generals, and Federal Regulation of Bitcoin." *Journal of Taxation & Regulation of Financial Institutions* **27**(4).
Loader, I. and N. Walker (2004). "State of Denial? Rethinking the Governance of Security." *Punishment & society* **6**(2): 221–228.

DOI: 10.1057/9781137399052.0009

Lumby, A. (2013). "Porn, Drugs, Hitmen, Hackers: This Is the Deep Web." *The Fiscal Times*.

Magura, S. (2012). "Failure of Intervention or Failure of Evaluation: A Meta-Evaluation of the National Youth Anti-Drug Media Campaign Evaluation." *Substance use & misuse* **47**(13–14): 1414–1420.

Malm, A. and G. Bichler (2011). "Networks of Collaborating Criminals: Assessing the Structural Vulnerability of Drug Markets." *Journal of Research in Crime and Delinquency* **48**(2): 271–297.

Markoff, J. (2005). *What the Dormouse Said: How the Sixties Counterculture Shaped the Personal Computer Industry*, London, Penguin.

Martin, J. (2013). "Informal Security Nodes and Force Capital." *Policing and Society* **23**(2): 145–163.

Martin, J. (2013). "Lost on the Silk Road: Online drug distribution and the 'cryptomarket'." *Criminology and Criminal Justice*: 1748895813505234.

Masten, S. V. and G. V. Guenzburger (2014). "Changes in Driver Cannabinoid Prevalence in 12 US States after Implementing Medical Marijuana Laws." *Journal of Safety Research* **50**: 35–52.

May, T. (2001). "Crypto Anarchy and Virtual Communities." *Crypto Anarchy, Cyberstates, and Pirate Utopias.* Cambridge, Massachusetts, MIT Press, 65–79.

Miron, J. and K. Waldock (2010). *The Budgetary Impact of Ending Drug Prohibition*. Washington D.C., Cato Institute.

Moreno, C. (2014). "Homer Simpson Is 'El Chapo' In Prophetic Drug War Art Series." *The Huffington Post*.

Morris, S. D. (2013). "The Impact of Drug-Related Violence on Corruption in Mexico." *The Latin Americanist* **57**(1): 43–64.

Morselli, C., et al. (2007). "The Efficiency/Security Trade-Off in Criminal Networks." *Social Networks* **29**(1): 143–153.

Moses, A. (2013). "Underweb Anger as Silk Road Seller Does a Runner." *Sydney Morning Herald*. Sydney, Fairfax.

Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System." *Consulted* **1**: 2012.

Natarajan, M. (2006). "Understanding the Structure of a Large Heroin Distribution Network: A Quantitative Analysis of Qualitative Data." *Journal of Quantitative Criminology* **22**(2): 171–192.

NCA (2013). NCA Arrests Silk Road Suspects, National Crime Agency.

DOI: 10.1057/97811373990520009

Nutt, D. (2012). "Drugs Without the Hot Air." *Minimising the Harms of Legal and Illegal Drugs.* Cambridge: Cambridge UIT.

O'Neill, P. (2013). "Atlantis: The Online Black Market for the Masses." *The Daily Dot*.

O'Neill, P. (2014). "The Final Confessions of a Silk Road Kingpin." *The Daily Dot*.

Orizio, G., et al. (2011). "Quality of Online Pharmacies and Websites Selling Prescription Drugs: A Systematic Review." *Journal of Medical Internet Research* **13**(3).

Ormsby, E. (2012). The Drug's in the Mail. *The Age*. Melbourne, Fairfax.

Ormsby, E. (2013). Interview with a (virtual) drug tsar. *All Things Vice*. **2014**.

Ormsby, E. (2013). Remember, Remember… Silk Road redux. *All Things Vice*.

Palmer, A. (2012). "Deep Web: Drugs, Guns, Assassins, Jet Planes All for Sale on Vast Anonymous Network." *The Mirror*.

Payan, T. (2006). *Cops, Soldiers, and Diplomats: Explaining Agency Behaviour in the War on Drugs*. Lanham, MD, Lexington Books.

Provos, N., et al. (2009). "Cybercrime 2.0: When the Cloud Turns Dark." *Communications of the ACM* **52**(4): 42–47.

Quigley, J. (2013). "Deep Web" Drug Peddling Site Atlantis Begins Advertising Push. *The Diplomat*.

Ritter, A. (2006). "Studying Illicit Drug Markets: Disciplinary Contributions." *International Journal of Drug Policy* **17**(6): 453–463.

Ritter, A., et al. (2012). *Evaluating Drug Law Enforcement Interventions Directed Towards Methamphetamine in Australia*, National Drug Law Enforcement Research Fund (NDLERF).

Rose, S., et al. (2011). "Online Customer Experience: A Review of the Business-to-Consumer Online Purchase Context." *International Journal of Management Reviews* **13**(1): 24–39.

Ross, W. (2013). "So Long, Silk Road." *New York Daily News*. 30/5/2014

Rubens, P. (2013). "Silk Road: Will Cybercrime Evolve in Wake of Takedown?" *BBC*.

Schneier, B. (2013). "Attacking Tor: How the NSA Targets Users' Online Anonymity." *The Guardian*, Guardian News and Media Limited.

Shearing, C. and J. Wood (2003). "Nodal Governance, Democracy, and the New 'Denizens'." *Journal of Law and Society* **30**(3): 400–419.

Sjouwerman, S. (2011). *Cyberheist*, KnowBe4 LLC.

DOI: 10.1057/9781137399052.0009

Solon, O. (2013). Police Crack Down on Silk Road Following First Drug Dealer Conviction. *Wired.co.uk*.

Steffen, G. and S. Candelaria (2012). *Drug Interdiction: Partnerships, Legal Principles, and Investigative Methodologies for Law Enforcement*, Florida, CRC Press.

Subramanian, R. and R. Moreno (2014). "Drug War Détente? A Review of State-level Drug Law Reform, 2009–2013."

Thaxter, K. (2010). "Cyber Bullying: Challenges and Strategies Faced by Juvenile Police Officers." *Journal of Social Sciences (15493652)* 6(4).

Trautman, L. J. (2014). "Virtual Currencies: Bitcoin & What Now after Liberty Reserve and Silk Road?" *Available at SSRN 2393537*.

Van Buskirk, J., et al. (2014). Drugs and the internet. *The National Illicit Drug Indicators Project*, National Drug and Alcohol Research Centre. **2.**

Van Hout, M. C. and T. Bingham (2013). "Responsible Vendors, Intelligent Consumers: Silk Road, the Online Revolution in Drug Trading." *International Journal of Drug Policy*.

Volkov, V. (2002). *Violent Entrepreneurs: The Use of Force in the Making of Russian Capitalism*, Cornell University Press.

Wall, D. (2001). *Crime and the Internet*, London, Routledge.

Wall, D. (2007). *Cybercrime: The Transformation of Crime in the Information Age*, Polity.

WCO (2013). Illicit Trade Report 2012. W. C. Organisation.

Weinstein, L. (2008). "Mumbai's Development Mafias: Globalization, Organized Crime and Land Development." *International Journal of Urban and Regional Research* **32**(1): 22–39.

Whitehead, L. (2013). "Father Devastated by Son's Overdose Angered by Online Marketplace for Drugs." *ABC News*, Australian Broadcasting Corporation.

Williams, M. (2007). "Cyber-Crime on the Move." *Displacing Place: Mobile Communication in the Twenty-first Century* **42**: 91.

Wood, J. and B. Dupont (2006). *Democracy, Society and the Governance of Security*, Cambridge, Massachusetts, Cambridge University Press.

Xu, J. and H. Chen (2008). "The Topology of Dark Networks." *Communications of the ACM* **51**(10): 58–65.

Zetter, K. (2014). New 'Google' for the Dark Web Makes Buying Dope and Guns Easy. *Wired*, Wired.com.

DOI: 10.1057/97811373990520009

Index

DOI: 10.1057/97811373990520010

DOI: 10.1057/9781137399052.0010