An Investigation of Cryptomarkets: Assessing the Online Drugs Trade from the Perspectives of Australian Health and Law Enforcement Agencies

A thesis submitted to the Department of Policing, Intelligence and Counter Terrorism, Faculty of Arts at Macquarie University for the degree of Master of Research

November 2014

By Romal Nasseri

Abstract

The development of cryptomarkets is a new criminological phenomenon. Cryptomarkets are defined as a platform that operates on an encrypted part of the Internet and enables its users to anonymously communicate and conduct illicit transactions. This research analyses cryptomarkets through current Australian drug policy. The findings of this research reveal that different organisations such as law enforcement agencies and the Australian Institute of Health and Welfare have different perspectives and priorities when exploring the operations of cryptomarkets. These agencies often have contradictory views when analysing drug-related issues through current Australian drug policy, as they have different agendas on how those issues should be addressed. From the perspective of law enforcement agencies, it is necessary to disrupt the infrastructure of cryptomarkets and prevent people from conducting illicit transactions. However, from the perspective of the Australian Institute of Health and Welfare, disrupting cryptomarkets would have negative consequences for the Australian Government and Australian communities. In conclusion, this research argues that although cryptomarkets are a transformative platform that enables individuals to conduct illicit transactions, they should not be disrupted because they offer a less violent alternative to conventional drug distribution networks.

Keywords

Drug distribution network, cryptomarket, cybercrime, Australian drug policy, harm reduction, systemic drug-related violence, War on Drugs

Table of Contents

Abstract ..... **i**

Keywords ..... **i**

Statement of Original Authorship ..... **iv**

Acknowledgements ..... **v**

Chapter 1: Introduction **1**
1.1 – Thesis 1
1.2 – Comparing Cryptomarkets with Traditional Illicit Drug Markets 3
1.3 – Background of the Project 5
1.4 – The Statement of Topic and Aims 8
1.4.1 – Research Questions 8
1.4.2 – Rationale 9
1.4.3 – Scope of the Project 9

Chapter 2: A Literature Survey of Cryptomarkets **11**
2.1 – Online Drug Market Themes 11
2.1.1 – Online Drug Markets from the Perspective of Cybercrime 12
2.1.2 – Online Illicit Marketplaces and the Cryptomarkets 17
2.1.3 – The Crypto-Currency of Cryptomarkets 19
2.1.4 – Conundrum for Law Enforcement and Postal Authorities 20
2.1.5 – Potential Interventional Strategies 22
2.1.6 – Violence Reduction 23
2.1.7 – Harm Reduction 25

Chapter 3: Methodology **27**
3.1 – Research Design of the Project 28
3.1.1 – Research Questions 28
3.1.2 – Method 29
3.1.3 – Data Analysis 31

Chapter 4: Analysis of Cryptomarkets through the Realm of Discourse Analysis **32**
4.1 – Discourse Analysis of Cryptomarkets 32
4.1.1 – Language Used by Commentators to Describe Cryptomarkets 33
4.1.2 – Perspective of Law Enforcement Officials on Cryptomarkets 35
4.1.3 – Scholarly Perception of Cryptomarkets 37
4.1.4 – Conclusion 40

Chapter 5: Analysis of Cryptomarkets **42**
5.1 – The Impact of Cryptomarkets on Contemporary Society 42
5.1.1 – Harm Reduction through Cryptomarkets and Online Forums 43
5.1.2 – The Link between Australian Drug Policy and Cryptomarkets 46
5.1.3 – Violence Reduction through Cryptomarkets. 50
5.1.4 – Conclusion 54

Chapter 6: Targeting Cryptomarkets **55**
6.1 – Potential Interventional Strategies 55
6.1.1 – Disrupting the TOR Network 56
6.1.2 – Disrupting the Financial Infrastructure 58
6.1.3 – Disrupting the Delivery Model 59

6.1.4 – Undercover Investigation 62
6.1.5 – Laissez-faire 64
6.1.6 – Conclusion 65

Chapter 7: Unintended Side Effects of Targeting Cryptomarkets 67
7.1 – Ramifications of Disrupting Cryptomarkets 67
7.1.1 – Likely Impact of Targeting Cryptomarkets 69
7.1.2 – Conclusion 71

Chapter 8: Conclusions and Future Directions 73
8.1 – Research Findings 73
8.1.1 – Limitations of the Project 77
8.1.2 – Future Work 78

References 79

Statement of Original Authorship

This thesis is submitted to Macquarie University in fulfillment of the requirement for the Degree of Master of Research.

This thesis represents my own work and contains no material which has been previously submitted for a degree or diploma at this University or any other institution, except where acknowledgement is made.

Acknowledgements

I would like to use this opportunity to express my deep gratitude to everyone who supported and encouraged me throughout the course of this research. I am indebted to my supervisor Dr James Martin for his insightful and encouraging comments and suggestions throughout this research. I owe thanks to Dr Noah Bassil for his continuous encouragement and support at all decisive stages of this research. I would like to thank the two anonymous examiners for their significant contribution to this research. My sincere thanks goes to the Faculty of Arts, in particular the department of Policing, Intelligence and Counter Terrorism at Macquarie University. Finally, extra special thanks to my family and friends, in particular my brother Dr Emal Nasseri, and my best friend Maryiam Issa Farzam for their constant support and encouragement.

Chapter 1: Introduction

1.1 – Thesis

In this new era of global communication, the Internet is often viewed as a democracy-building technology, as it allows voiceless individuals the opportunity to be heard in the public arena (Barratt et al., 2013, p. 3; Leaning, 2009). According to Barak and King (2000, p. 517), the Internet has two faces, positive and negative. Its positive aspect is that the Internet enables the enrichment and improvement of human functioning in many areas, including communication, education, health, commerce, and entertainment. In its negative aspect, the Internet may create a threatening environment and expose people to great risks such as breaking and separating families, cheating on spouses, accessing private documents and secrets, stealing money, and making people commit suicide (Barak and King, 2000, p. 517). The negative aspect of the Internet is often understood as it being a platform that hosts a wide range of crimes (Barak and King, 2000). From a criminological standpoint, the negative aspects of the Internet may include new waves of crime such as cyber stalking, cyber bulling, Internet fraud, child pornography, and, more importantly for the purpose of this study, the online illicit drug trade.

However, empirical evidence (Barratt et al., 2013) suggests that online illicit drug websites may not easily be classified as 'negative' as one may first expect. This is due to the fact that online illicit drug sites assist a number of government organisations such as public health and educational institutions (e.g., schools, universities, drug education programs). According to Barratt et al. (2013), if the

online illicit drug market is analysed from the perspective of public health and educational institutions, it is a transformative platform that allows individuals to anonymously disseminate drug-related information and educate drug-users on how to minimise drug-related harm.

Considering the argument provide by Barratt et al. (2013), the online illicit drug market is a positive or negative (depending on one's perspective) development that enables individuals to freely and anonymously consume, produce and disseminate detailed drug-related information and conduct numerous illicit transactions (Martin, 2014; Barratt et al., 2014; Aldridge and Decary-Hetu, 2014; Van Hout and Bingham, 2013; Martin, 2013; Van Hout and Bingham, 2013a; Barratt et al., 2013; Van Hout and Bingham, 2013b; Christin, 2012; Barratt, 2012).

Online drug distribution varies significantly from conventional forms of drug distribution. This is due to the fact that drug-users have access to a worldwide market, obtain and produce up-to-date drug-related information and conduct anonymous transactions via the Internet (Barratt et al., 2013). The argument provided by Barratt et al. (2013) suggests that online drug distribution is a concerning issue for governments and law enforcement agencies around the world, as it is changing the nature of the illicit drug trade. At the present time, governments and law enforcement authorities are struggling to prevent individuals from engaging in online drug-related discussions, disseminating detailed drug-related information, and most significantly distributing and purchasing illicit goods (Martin, 2014; Barratt et al., 2014; Aldridge and

Decary-Hetu, 2014; Van Hout and Bingham, 2013; Martin, 2013; Van Hout and Bingham, 2013a; Barratt et al., 2013; Van Hout and Bingham, 2013b; Christin, 2012; Barratt, 2012). The reason behind this struggle is that the operations of online illicit drug sites are conducted on the 'dark net'. The dark net is dependent upon encrypted technologies such as the TOR (The Onion Router) network and Bitcoin (encrypted electronic currency) (Phelps and Watt, 2014; Aldridge and Decary-Hetu, 2014; Martin, 2014; Barratt et al., 2014; Martin, 2013; Barratt, 2012).

Like Aldridge and Decary-Hetu (2014), Martin (2014), Barratt et al. (2014), Martin (2013) and Barratt (2012), this research project also refers to online illicit drug sites as dark net marketplaces or *cryptomarkets.* A cryptomarket is defined as "an online forum where goods and services are exchanged between parties who use digital encryption to conceal their identities" (Martin, 2013, p. 6). This suggests that cryptomarkets differ from other types of online illicit market, as they predominantly rely on encrypted technologies to conduct illicit transactions. According to Martin (2013, p. 6), cryptomarkets share a range of characteristics such as reliance on the TOR network, use of cryptonyms to conceal user identity, use of traditional postal systems to deliver goods, third-party hosting and administration, decentralised exchange networks and use of encrypted electronic currency or 'cryptocurrencies' (e.g., Bitcoin).

1.2 – Comparing Cryptomarkets with Traditional Illicit Drug Markets

While cryptomarkets differ significantly from traditional illicit drug market, there are numerous identical aspects of the two markets. In order to provide a

systematic overview of cryptomarkets, it is significantly important for governments, law enforcement agencies and criminologists to compare aspects of both traditional and online drug markets. This would allow governments, policing authorities and criminologists to critically annalyse and identify how similar and distinct cryptomarkets are from the traditional illicit drug markets. For instance, both online and offline drug markets have primary goals, and that is to distribute illicit goods and maintain market shares. While both of these illicit drug markets use different methods, they share similar ambitions (i.e., distributing illicit goods) (Aldridge and Decary-Hetu, 2014; Van Hout and Bingham, 2013; Martin, 2013; Van Hout and Bingham, 2013b; Christin, 2012).

Moreover, both traditional and online illicit drug markets distribute and ship their products to a worldwide market. Due to the expansion of international trade (i.e., globalisation), increased number of passengers travelling through borders, and the huge volume of mail, it is significantly difficult for governments and law enforcement agencies, in particular customs and border protection agencies to intercept illicit commodities (Martin, 2014; Aldridge and Decary-Hetu, 2014; Van Hout and Bingham, 2013; Barratt et al., 2013; Van Hout and Bingham, 2013b; Martin, 2013; Christin, 2012; Jenner, 2011). According to Jenner (2011), it is impossible for authorities to know the exact amount of drugs that are slipping through the cracks. However, there are a number of studies (Bush et al., 2004; Duff, 2004) suggesting that, each year, the Australian customs and border protection authorities intercept only 10–20% of the illicit drugs that are imported into the country. When police intercept illicit

drugs, whether the drugs belong to traditional drug markets or cryptomarkets, they often use traditional policing techniques, and they are as follows:

- Disrupting networks
- Disrupting financial infrastructure
- Disrupting delivery process
- Undercover investigation

These traditional policing strategies will be discussed in Chapter 6, and how they tend to be problematic when policing cryptomarkets.

1.3 – Background of the Project

The first online illicit market, *Famer's Market*, was launched in 2006. Over half a decade after the launch of *Farmer's Market*, cryptomarkets started their operations (Martin, 2014). According to Phelps and Watt (2014) and Christin (2012), the cryptomarket Silk Road has been operating since February 2011. The establishment of this new breed of drug market attracted worldwide media. Numerous media articles (see, for example, Swearingen, 2014; Power, 2013; Ormsby, 2012; Pauli, 2012; Moses, 2012) began to surface, warning people about the dangers associated with this lucrative drug market and also noting that law enforcement agencies are struggling to prevent or minimise individuals from distributing or obtaining illicit goods via the Internet (Martin, 2014; Martin, 2013). The main reason that law enforcement agencies are struggling to target or minimise cryptomarkets is the fact that they operate on the "dark net". The dark net is the encrypted part of the Internet that allows people to anonymously communicate and exchange illicit goods. This anonymity prevents law

enforcement agencies to identify people who participate or exchange illicit goods in these illicit drug bazaars. Another issue for law enforcement agencies is that cryptomarkets are hosted by third party administrators who obtain a percentage of each transaction conducted. Third party hosting provides encrypted walls for administrators, distributors and consumers of these sites to avoid being traced by law enforcement agencies (Martin, 2014; Barratt et al., 2014; Aldridge and Decary-Hetu, 2014; Van Hout and Bingham, 2013; Martin, 2013, p. 2; Van Hout and Bingham, 2013a; Barratt et al., 2013; Van Hout and Bingham, 2013b; Christin, 2012; Barratt, 2012).

Accessing Cryptomarkets: in order to access cryptomarkets, individuals are required to use digital encrypted technologies (e.g., TOR) to hide their IP addresses (the code assigned to each computer on the Internet) and the physical location of their servers (Aldridge and Decary-Hetu, 2014; Barratt et al., 2013). The TOR network is a freely available service that guarantees the anonymity of its participants. Before accessing these anonymous illicit drug sites, a buyer needs to download and install TOR on his/her computer. After having TOR installed, the prospective buyer then needs to register with the website and create an account (Christin, 2012). Following the registration process, the buyer is presented with the front page of the website and can access the list of illicit drugs (Barratt et al., 2013; Christin, 2012).

Purchasing Process: after obtaining the list of illicit goods available on the site, the buyer can purchase any type of drug, depending upon availability. While TOR offers communication anonymity, cryptomarkets need to also preserve

payment anonymity (Christin, 2012, p 4). Cryptomarkets support encrypted currencies such as Bitcoin, Litecoin and Peercoin (Ren, 2014; Martin, 2014; Barratt et al., 2014; Aldridge and Decary-Hetu, 2014; Van Hout and Bingham, 2013; Martin, 2013; Van Hout and Bingham, 2013a; Barratt et al., 2013; Van Hout and Bingham, 2013b; Christin, 2012; Barratt, 2012). These encrypted currencies are peer-to-peer, distributed payment systems that allow individuals to conduct online transactions without the need for a central third-party (Christin, 2012; Nakamoto, 2008). Before purchasing illicit goods through cryptomarkets, a buyer needs to procure Bitcoins, or other cryptocurrencies. Once a buyer procures Bitcoins, then he/she would be able to conduct anonymous transactions. In other words, at the end of each transaction, a buyer needs to use Bitcoin or an alternative currency to finalise his/her transaction (Ren, 2014; Christin, 2012).

Finalising: once a purchase has been made, the vendor needs a physical address to ship the illicit goods. To maintain anonymity, cryptomarkets continuously encourage drug-users to use a different address from their place of residence (e.g., a neighbour's residence, a dummy post box, a place of business or a vacant house) (Christin, 2012). Vendors then use the traditional postal system to dispatch goods to their nominated destinations. Upon receipt of an order, consumers leave feedback about the quality of goods and provide comments about the reliability of suppliers (Martin, 2013; Christin, 2012).

1.4 – The Statement of Topic and Aims

This research project is an exploratory work intended to analyse cryptomarkets from the perspectives of Australian health and law enforcement agencies. Hence, this research project has a number of aims and objectives and they are as follows:

- The first aim of this research project is to analyse cryptomarkets through the realm of discourse analysis and cybercrime. This allows the researcher to analyse and explore how certain groups (e.g., media, law enforcement agencies and academics) perceive cryptomarkets. It is critically important to achieve this aim, because cryptomarkets are often perceived and cited differently by certain groups.
- The second and central aim of this research project is to analyse cryptomarkets through current Australian drug policy.
- The next aim of this research project is to critically examine the role of law enforcement agencies in preventing people from conducting illicit transactions via the Internet and analyse the current online drug prevention strategies.
- The last aim of this research project is to measure the effectiveness of those existing online drug prevention strategies and also identify associated unintended consequences.

1.4.1 – Research Questions

This thesis focuses on four research questions, each with its own chapter:

1. How do media, law enforcement agencies and scholars perceive cryptomarkets?
2. Should law enforcement agencies disrupt or target cryptomarkets?
3. What strategies are available to prevent people from buying and selling illicit drugs through the Internet?
4. What might be the unintended side effects when disrupting or targeting cryptomarkets?

1.4.2 – Rationale

Academics such as Martin (2014), Barratt et al. (2014), Aldridge and Decary-Hetu (2014), Van Hout and Bingham (2013), Martin (2013), Van Hout and Bingham (2013a), Barratt et al. (2013), Van Hout and Bingham (2013b), Christin (2012), and Barratt (2012) claim that law enforcement agencies have had little impact in minimising the rapid proliferation of buyers and sellers populating cryptomarkets. The rationale behind this research project is to build a body of knowledge on the online illicit drug trade and the role of policing authorities. The findings emerging from this research will provide significant information and shed light on previously unknown aspects of cryptomarkets and what impact targeting these lucrative drug markets may have on society.

1.4.3 – Scope of the Project

It is important to clarify that this project analyses cryptomarkets only through current Australian drug policy. It is beyond the scope of this research project to examine and explore these online illicit bazaars through other Western (e.g.,

United Kingdom, France, Germany, Netherlands, America, Canada etc.) or indeed non-Western drug policies. It is also beyond the scope of this research project to examine and explore other illicit drug sites, as the main focus of this project is to analyse cryptomarkets.

Chapter 2: A Literature Survey of Cryptomarkets

Since the development of cryptomarkets, a small amount of research has been dedicated towards these new and lucrative drug markets. Cryptomarkets are changing the nature of drug distribution. Governments, policy makers, and law enforcement agencies are currently struggling to establish a definitive solution on how to permanently shut down these illicit drug bazaars and prevent people from buying and selling illicit drugs. There are, currently, a handful of researchers (Phelps and Watt, 2014; Martin, 2014; Aldridge and Decary-Het, 2014; Barratt et al., 2014; Van Hout and Bingham, 2013; Barratt, et al., 2013; Christin, 2012) exploring different facets of cryptomarkets and they have suggested that online criminal activities, in particular drug distribution, are continuing to expand. Buying and selling illicit goods is now feasible through the 'dark side' of the Internet. It is, therefore, of high importance to conceptualise the activities of cryptomarkets through the sphere of cybercrime and also explore how computer technologies allow individuals to conduct illicit transactions while remaining completely anonymous. The following sub-sections provide an overview of related work on cryptomarkets from various criminological perspectives.

2.1 – Online Drug Market Themes

For this research, the following seven themes of cryptomarkets have been identified.

2.1.1 – Online Drug Markets from the Perspective of Cybercrime

Since online illicit drug distribution networks are facilitated through computer technologies (i.e., computers, sophisticated software, etc.) and in particular the Internet, it is crucial to scrutinise online drug marketplaces from the perspective of cybercrime (Martin, 2013). While cybercrime has attracted the attention of numerous researchers around the world, several studies indicate that the primary problem in identifying and analysing cybercrime is the lack of a consistent current definition amongst scholars, government analysts, journalists and media pundits (Wall, 2001; Yar, 2005). For example, Wall (2001, p. 2) argues that the term 'cybercrime' has no specific referent in law. Scholars have defined cybercrime in a number of conflicting ways to make it applicable to their own research (Jaishankar, 2011). Thomas and Loader (2000, p. 3), for instance, define cybercrime as *"computer mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks"*. However, a recent study conducted by Jaishankar (2011) indicates that there is a problem in the definition of cybercrime provided by Thomas and Loader (2000). His 2011 book *Cyber Criminology* suggests that the study of Thomas and Loader (2000) is considered to be out of date and it does not provide a recent perspective of cybercrime.

According to Jaishankar (2011), since cybercrime is dependent on the Internet and computer technologies, scholars should regularly redefine it. It is argued by Jaishankar (2011) that the Internet and computer technologies are advancing on a regular basis and, as a direct consequence of those advancements, new forms of cybercrime tend to emerge. Thus, scholars should reinterpret the definition of

cybercrime on a regular basis and provide more up-to-date scholarly perspectives on new forms of cybercrime (Jaishankar, 2011). First, in order to appreciate and redefine various aspects of cybercrime, scholars should make a distinction between 'computer crime' and 'cybercrime'. While the former does not require an individual to possess special computer skills, the latter requires highly sophisticated computer networks and computer skills (Jaishankar, 2011).

Interestingly, the studies of Wall (2007) and Yar (2005) also support the claims made by Jaishankar (2011). Their studies (Wall, 2007; Yar, 2005) have identified a variety of typologies to assist in analysing cyber or computer-related offences. Yar (2005, p. 409), for instance, asserts that there are two distinct classifications such as 'computer-assisted' and 'computer focused' cybercrimes that assist scholars in analysing cyber or computer-related offences. Computer-assisted cybercrimes refer to those 'traditional' forms of offences that existed before the advent of the Internet and have been reinvented by modern computer technologies, which include theft, fraud, bullying, racism and defamation (Jaishankar, 2011; Jewkes and Yar, 2010; Grabosky, 2007; McCusker 2007; Furnell, 2002). Grabosky (2001) also offers specific commentary on this point, suggesting that computer-assisted cybercrimes are not unique to the online world. In fact, they are described as *'old wine in new bottles'*. Thus, computer-assisted offences *"have the familiar ring of the 'traditional' rather the 'cyber' about them"* (Wall 2010, p. 77). Considering those aforementioned claims made by Grabosky (2001) and Wall (2010), computer crimes fall under the category of computer-assisted cybercrime (Jaishankar, 2011, p. 230).

Computer focused cybercrimes, on the other hand, are linked with 'new' types of offences that have evolved through the use of sophisticated computer technologies and examples include illegal accessing (hacking) of personal computers, interrupting, damaging and deleting useful information, developing malicious software (i.e., malicious codes, worms, viruses, Trojans), and hijacking of infected computers (Jewkes and Yar, 2010; Harper and Frailing, 2010). An ever-growing body of research suggests that these forms of offending came into existence soon after the advent of computer technologies (Balkin et al., 2006; Zheng et al., 2003; Quarantiello, 1997). Another scholar who analysed different forms of cybercrime is Furnell. His 2002 book *Cybercrime: Vandalizing the Information Society* suggests that computer focused cybercrimes are considered to be unique to the online world, as these forms of offences were not conceivable merely two decades back and they have now become facts of life.

Despite having identified these typologies (computer-assisted and computer focused), there are limitations when conceptualising the activities of online drug markets through the sphere of cybercrime. For instance, it seems logical to classify online illicit drug distribution as computer-assisted as opposed to computer focused. This is because the sale and distribution of illicit drugs were long established and now facilitated by the Internet and other sophisticated computer technologies. However, the study conducted by Martin (2013, p. 4) maintains that *"when considering this classification in further depth, the foundational dichotomy between computer-assisted and -focused cybercrimes begins to break down"*. The main reason behind this breakdown is that online

illicit drug distribution involves a wide range of novel and conventional offences that are facilitated by computer technologies (Martin, 2014; Martin, 2013). This implies that the activities of online illicit drug markets should also be classified as computer focused rather than computer-assisted cybercrimes, as certain aspects (i.e., conducting illicit transactions) of online drug marketplaces are dependent on the Internet, and other sophisticated computer technologies (i.e., TOR network) (Martin, 2014; Martin 2013). The aforementioned arguments suggest that there are deficiencies associated with the classification of computer-assisted and computer focused cybercrimes.

Wall (2007) acknowledges those deficiencies and offers a 'transformation test' that reviews computer-related offences according to their integration with online networks. Illustrating the logic of the transformation test and the critical link between networks and cybercrime, Wall (2007, p. 34) argues that the defining characteristics of cybercrime are supported by networked technologies. The test of cybercrime must emphasise what is left behind if the involvement of those networked technologies is removed.

Based on Wall's (2007) transformation test, cybercrime can be categorised into numerous generations and two of those generations are relevant for analysing illicit drug websites (Martin, 2014; Martin, 2013). Wall (2007) argues that the 'first-generation' of cybercrimes are considered similar to computer-assisted offences, because computer networks solely facilitate offences that are categorised under the first-generation of cybercrimes. If the involvement of computers and online networks are eliminated from the equation, then first-

generation offences will persist by other means. These forms of offences are committed independently. This suggests that cyber-offenders do not need large networks to commit first-generation cybercrimes if the involvement of computer technologies is removed (Wall, 2007).

By contrast, second-generation cybercrimes involve the use of global information networks that offer a wide range of illicit opportunities. Wall (2007) argues that if one could imagine eliminating computers and associated online networks from the equation, then second-generation offences may still persist but only at an extremely low rate, as these types of offences need large networks that can only be carried out through modern computer technologies (Martin, 2013, Wall, 2007).

Despite having these sophisticated typologies, scholars are still struggling to conceptualise the activities of online illicit drug markets through the lens of cybercrime. It is immensely complicated to categorise online illicit drug distribution under one specific classification. In fact, they should be categorised under multiple generations of cybercrime. This is due to the fact that the activities of online drug markets have a tendency to adhere to various generations of cybercrime (Martin, 2013, p. 5). For instance, if the involvement of computer networks is eliminated from online illicit drug markets, then sale and distribution of illicit goods will persist by other means (i.e., traditional forms of drug distribution). However, in this case, it would need large criminal networks (i.e., importers, wholesalers and street-level dealers) to distribute illicit drugs without the use of computer networks (Martin, 2013).

According to Martin (2013), online illicit drug markets involve novel and conventional offences of sale and trafficking of illicit goods and they rely on online distribution networks. This process varies from traditional forms of illicit exchange. Martin (2013, p. 6) argues that:

> In the same way that the global operations of eBay and Amazon market differ significantly from local trading marketplaces, so too do the operations of online drug markets differ from those of traditional drug distributors and street dealers. This difference is not adequately reflected in existing cybercrime typologies. This suggests the need for a new form of conceptualization to capture the particular features inherent to online illicit drug markets.

2.1.2 – Online Illicit Marketplaces and the Cryptomarkets

Considering those previously mentioned limitations pertaining to the conceptualisation of online drug markets as cybercrime, as an alternative it may be helpful to view them as specific types of online drug markets, in particular as cryptomarkets (Martin, 2014; Aldridge and Decary-Hetu, 2014; Barratt et al., 2014; Martin, 2013). A cryptomarket is defined as *"an online forum where goods and services are exchanged between parties who use digital encryption to conceal their identities"* (Martin, 2013, p. 6). Taking that into account, several other studies (Barnet, 2014; Christin, 2012) suggest that cryptomarkets have particularly favoured those individuals who seek to participate in some sort of cybercrime activities. Barnet's recent publication (Barnet 2014) *Virtual Currencies: Safe for Business and Consumers or Just for Criminals* argues that cryptomarkets have offered thousands of drug dealers and other unlawful vendors to distribute thousands of kilograms of illicit drugs while remaining

completely anonymous. These drug markets not only allow individuals to participate in exchanging illicit drugs, they also offer individuals the opportunity to participate in a number of other types of illegal activities (Christin, 2012). This suggests that while cryptomarkets mainly specialise in illicit drug distribution, they also tend to deal in other black market goods and services. The study of Christin (2012, p. 2) argues that *"online drug marketplaces very often specialize in 'black market' goods, such as pornography, weapons or narcotics"*.

The study conducted by Van Hout and Bingham (2013) contradicts the claim made by Christin (2012). Their study (Van Hout and Bingham 2013) indicates that cryptomarkets are in fact discouraging other forms of illicit activities. According to Van Hout and Bingham (2013), not all cryptomarkets, such as Silk Road, specialise in other black markets (i.e., fraud, counterfeit documents, child pornography etc.); in fact, Silk Road prohibits other forms of illicit activities that intend to harm or defraud individuals. In particular, the sales of child pornography and counterfeit documents are strictly prohibited. Van Hout and Bingham (2013) elaborate on illicit drug markets; however, they do not thoroughly address other non-drug-related services that these websites offer.

In comparison, the study of Martin (2013) provides a better argument suggesting that, in any case, whether cryptomarkets encourage or discourage non-drug-related criminal activities, there are other cryptomarkets that provide illicit goods and services. Just by a quick search through *Hidden Wikipedia* (another website accessible through the TOR network), individuals can access links to

numerous other cryptomarkets. These cryptomarkets offer a wider range of illicit goods, services and criminal activities, such as child pornography, counterfeit documents, money laundering, stolen credit cards, forged identity documents, hacking services, illegal firearms and ammunition, and extortion (Martin, 2013). It is deduced by Martin (2013) that these cryptomarkets tend to share the following characteristics: reliance on the TOR network, use of cryptonyms to conceal user identity, use of traditional postal systems to deliver goods, third-party hosting and administration, decentralised exchange networks and, more significantly, use of encrypted electronic currency (i.e., Bitcoin) (Martin, 2013, p. 6).

2.1.3 – The Crypto-Currency of Cryptomarkets

Cryptomarkets depend on encrypted electronic currency called Bitcoin (Barnet, 2014, Barratt et al., 2014). According to Nakamoto (2008, p. 1), *"it is a peer-to-peer version of electronic cash that allows online payments to be sent directly from one party to another without going through a financial institution"*. Barnet (2014) argues that Bitcoin is a non-government-controlled anonymous and untraceable crypto-currency, which was introduced in 2009 by Satoshi Nakamoto and offers its clients the opportunity to participate in some sort of online criminal activity (Basu, 2014; Van Hout and Bingham, 2013; Barratt et al., 2013).

The study presented by Nakamoto (2008) indicates that Bitcoin was developed with a positive intention to maintain people's privacy and allow parties to transact directly with each other without the need for a trusted third party. For

instance, Bitcoins are often exchanged between individuals who play online games. Here, the main priority is to maintain their privacy and allow them to conduct transactions with each other without the involvement of a financial institution (Phelps and Watt, 2014).

There are numerous other studies (Basu, 2014; Barnett, 2014; Barratt et al., 2014; Van Hout and Bingham, 2013) that refute the findings presented by Nakamoto (2008), suggesting that while Bitcoin may have been developed with positive intention, it facilitates a broad range of illicit activities that were previously not predicable. For example, since the development of cryptomarkets, Bitcoin is used as virtual money to buy illicit goods. Thus, it can be demonstrated that Bitcoin favoured those individuals who are willing to remain anonymous when conducting illicit transactions over the Internet (Barnett, 2014; Barratt et al., 2014; Van Hout and Bingham, 2013).

2.1.4 – Conundrum for Law Enforcement and Postal Authorities

The anonymity of Bitcoin and encrypted software (TOR network) has challenged law enforcement agencies in many ways (Van Buskrik et al., 2014; Van Hout and Bingham, 2013; Martin, 2013). One of the major challenges that law enforcement agencies are currently facing is that they are unable to identify who is buying or selling illicit drugs via cryptomarkets. This is due to the fact that TOR network promises its participants that their anonymity will be unchallenged by law enforcement agencies. However, there is empirical evidence suggesting that law enforcement agencies have other options to target and interrupt the operations of cryptomarkets (Barratt, 2012). Barratt (2012), for

example, states that what may potentially stop an exponential increase in the use of cryptomarkets is the problem of delivery. At the end of each transaction, a seller needs to physically dispatch goods to the nominated address that the buyer has provided. Sending illegal products between countries allows law enforcement agencies to interfere in the delivery process by seizing and intercepting packages and may potentially lead to the arrest of the would-be importer.

Meanwhile, the studies of Basu (2014), Van Hout and Bingham (2013b), Martin (2013) and Christin (2012) suggest that this strategy seems to be problematic, as there are numerous factors that prevent law enforcement agencies disrupting the delivery process. Martin (2013), for example, argues that one of the primary factors is that international trade is rapidly expanding, implying that more items are travelling through the international post than ever before. Examining merely a fraction of this considerable mail poses a significant challenge for customs and other law enforcement agencies. According to Martin (2013, p. 8), detecting and intercepting illegal items in this huge proportion of mail is like locating a needle in a haystack.

The issue associated with the studies of Martin (2013) and Van Hout and Bingham (2013b) is that they have identified factors that prevent law enforcement agencies to disrupt the delivery process; however, they do not offer any alternative solutions on how these issues can be addressed. The reason that Martin (2013) and Van Hout and Bingham (2013b) do not offer any solution may be the fact that cryptomarkets tend to reduce violence and may also

contribute in harm reduction. Hence, they argue that law enforcement agencies should not target these lucrative drug markets (Martin, 2013; Van Hout and Bingham, 2013). Christin (2012) has also conducted a similar study. Christin (2012) argues that while illicit drug sites may reduce violence, there are a number of drug prevention strategies that may help law enforcement agencies to effectively disrupt the activities of cryptomarkets.

2.1.5 – Potential Interventional Strategies

Law enforcement agencies have a strong interest in disrupting cryptomarkets and/or websites that deal with illicit drugs or drug-related information (Barratt et al., 2013; Christin, 2012). To date, they have been unsuccessful. Thus, a wide range of intervention strategies have been identified that may help law enforcement agencies to disrupt or target cryptomarkets and prevent drug-users from engaging with and buying illicit goods via the Internet. However, the problem associated with the study of Barratt, et al. (2013) is that they provided a brief summary on how governments and policing authorities can interrupt those illicit websites that distribute and promote illicit goods and services, whereas Christin (2012) presents a significant number of drug interventional strategies that may allow law enforcement agencies to permanently shut down such cryptomarkets or websites and other black markets.

On the contrary, various other studies (Spear, 2014; Mclntyre, 2014; Barratt et al., 2013, Van Hout and Bingham, 2013; Martin, 2013) suggest that none of those interventional strategies that were identified by Christin (2012) are effective. They argue that those interventional strategies are costly, complicated

and more importantly difficult to implement. According to Van Hout and Bingham (2013) and Martin (2013), cryptomarkets distribute a small amount of illicit goods compared to the global trade of illicit drugs. Spending a large sum of money to investigate a small amount of illicit drugs would not be an effective approach. In addition, if governments and policing authorities adopt any type of drug interventional strategy to block these lucrative drug markets, then drug-related discussion would go underground and, instead, traditional drug distribution would take place (Martin, 2014; Barratt et al., 2013; Van Hout and Bingham, 2013).

Alternatively, Van Hout and Bingham (2013), Martin (2013), Van Hout and Bingham (2013b), and Barratt et al. (2013) have suggested that the ultimate and most cost-efficient approach for governments and law enforcement agencies is not to interfere at all. This approach is not only cost-efficient, it also seeks to educate those individuals who are using illicit drugs (Christin, 2012). Interestingly, this notion is also supported by Barratt et al. (2013), Martin (2013), Van Hout and Bingham (2013), and Barratt (2012) who concluded that this new breed of illicit drug market has significantly benefited drug-users since they provide useful drug-related information and also tend to reduce drug-related violence.

2.1.6 – Violence Reduction

Empirical studies have found that cryptomarkets may play a crucial role in reducing systemic drug-related violence (Martin, 2014; Van Hout and Bingham, 2013b; Barratt et al., 2013; Martin, 2013; Van Hout and Bingham, 2013;

Christin, 2012; Werb et al., 2011). According to Martin (2013), cryptomarkets allow buyers and sellers to conceal their true identities and they (buyers and sellers) never meet face-to-face, nor, often, reside in the same country. *"This offers users the significant benefit of reducing the possibility of violence associated with 'in-person' forms of illicit exchange"* (Martin, 2013, p. 3). Similarly, Van Hout and Bingham (2013), Barratt et al. (2013) and Van Hout and Bingham (2013b) also argue that the anonymity of sellers and vendors may help reduce the risk of street violence. It is deduced by Van Hout and Bingham (2013b, p. 189) that the illicit drug industry represents a key cause of violence, particularly in urban settings and especially as a means for individuals and groups to secure and maintain market share. Cryptomarkets seem to present distributors and consumers with a novel way to avoid systemic drug-related violence and create distance amongst distributors and buyers (Van Hout and Bingham 2013; Barratt et al., 2013; Van Hout and Bingham 2013b). While there are numerous studies (Van Hout and Bingham, 2013; Barratt et al., 2013; Van Hout and Bingham, 2013b) providing an insight on cryptomarkets, there seems to be a lack of *detailed* overview of drug-related violence.

Hence, the study conducted by Werb et al. (2011) is widely appreciated by scholars who seek to investigate the relation between illicit drug markets and violence, as their primary research questions were specifically concerned with drug-related violence, in particular systemic violence. Werb et al. (2013) argue that illicit drug market violence is a major issue in contemporary society and it is continuing to expand in major cities due to gang-related violence. Reuter (2009) reaches similar conclusions to that of Werb et al. (2013). Reuter (2009) asserts

that illicit drugs, in general, trigger high levels of violence amongst organised crime groups. This is due to the fact that organised crime groups want to dominate the illicit drug market and compete with other gangs. Martin (2013) argues that cryptomarkets tend to reduce systemic drug-related violence and actively promote harm reduction.

2.1.7 – Harm Reduction

There are a number of studies exploring the relationship between cryptomarkets and harm reduction (Martin, 2014; Martin 2013; Van Hout and Bingham, 2013; Barratt et al., 2013; Barratt, 2012a). The findings of these studies seem to be unanimous. They all have presented evidence that cryptomarkets provide useful instruction and help to educate drug users about the risk associated with certain drugs. The analysis of Van Hout and Bingham (2013) has emphasised and reviewed a single case study, where they conducted an interview with an individual that recently participated in an online forum. Van Hout and Bingham (2013) argue that cryptomarkets, in particular public forums, are in fact discouraging potentially harmful dissemination of information, provide detailed instructions on drug use and educating drug users about the risk associated with illicit drugs. While Van Hout and Bingham (2013) presented interesting findings, there are certain limitations associated with the methodology used in their research. Van Hout and Bingham (2013) have interviewed and studied a single case study. Had the researchers included a greater number of participants in the interview, the validity of their findings would have been improved and their research outcome could have been extrapolated to a larger research community.

In comparison, the analysis and findings of Barratt (2012a) are appreciated and perhaps more widely applicable in the field of online illicit drug markets. Barratt (2012a) has interviewed and surveyed a significant number of drug users, moderators and administrators who recently participated in online drug discussion. According to Barratt et al. (2013) and Barratt (2012a), online drug forums play a pivotal role in reducing harm by instructing individuals on how to use drugs more safely and how to avoid bad experiences with drugs. In addition, the quantitative data presented by Barratt (2012a) also suggests that individuals participate in online drug-related discussion purely for the purpose of reducing harm and preventing unpleasant experiences with drugs. The following studies (Barratt, 2012a; Barratt et al., 2013; National Drug Research Institute, 2011), therefore, have concluded that cryptomarkets should be viewed from a public health perspective, as they actively seek to promote harm reduction and disseminate detailed drug-related information. Additionally, cryptomarkets help drug-users to access more comprehensive and relevant information than is available elsewhere. It can be demonstrated that the aim of these lucrative drug markets is not only to distribute illicit goods, they also seek to reduce drug-related harm, promote effective and safe methods to use drugs, and more importantly allow individuals to communicate and disclose personal experiences, stories and opinions in public forums (Martin, 2013; Barratt et al., 2013).

Chapter 3: Methodology

Methodology is the systematic, theoretical analysis of the methods applied to a field of study. In this research it is one of the fundamental elements of the project that provided the researcher with an insight on methods of data collection and techniques for analysing the collected data (O'Leary, 2004). There are two primary research methods available that can be adopted for this type of research. They are (1) qualitative and (2) quantitative. The former is concerned with people's views and attitudes about a particular research question and/or topic of interest in a non-numerical way (Seamon, 1999), while the latter seeks answers to a research question by examination of numerical data collected (Perry et al., 2000). While it is of high importance to select the most appropriate method for research, the validity of the study and its results is equally important. The results emerging from a research should have good external validity (i.e., the degree of generalisability of the results emerging from a study).

Initially, the researcher selected a mixed method approach to obtain primary data from the Australian Federal Police, Department of Policing, Intelligence and Counter Terrorism in Macquarie University and gain new information regarding this new breed of drug trade. By adopting a mixed method approach, the researcher planned to collect primary qualitative (interviews) and quantitative (surveys) data. However, the primary supervisor declined this methodological approach. This is due to the fact that such a methodological approach requires a significant amount of time to obtain and analyse the collected data. Obtaining ethical approval was also a major issue. Another major issue was that the data collection process would take several months, and the

analysis process would also require a significant amount of time to interpret the collected data before drawing conclusions. As mentioned earlier, to overcome these obstacles, the researcher changed the initial research design.

3.1 – Research Design of the Project

This project involves secondary data analysis. The aim of secondary data analysis is to address research questions that are distinct from that which the dataset was originally collected (Hewson, 2006). This suggests that the researcher has addressed the primary research questions by analysing and reinterpreting the existing data that were previously collected by other researchers. Such an approach seems to fit appropriately with this research, as its limitation seems to be fairly minimal (Bryman, 2008). This research design (secondary data analysis) helped the researcher to: (1) build a body of knowledge regarding the illicit nature of cryptomarkets; (2) obtain other researchers' perspectives on the topic of interest (online drug distribution); (3) build an appreciation of other researchers' methodological approaches who have previously analysed different facets of cryptomarkets; (4) identify an appropriate theoretical framework for this research project; and (5) most significantly, answer the primary research questions.

3.1.1 – Research Questions

The primary questions formulated for this research are as follows:

1. How do media, law enforcement agencies and scholars perceive cryptomarkets?

2. Should law enforcement agencies disrupt or target cryptomarkets?
3. What strategies are available to prevent people from buying and selling illicit drugs through the Internet?
4. What might be the unintended side effects when disrupting or targeting cryptomarkets?

3.1.2 – Method

The following steps have been used to select a research design, identify suitable theoretical frameworks, collect data and answer the primary research questions.

1) *Literature Review:* in order to conduct a thorough literature review, the researcher identified a number of key themes relevant to cryptomarkets, including: (1) online drug markets from the perspective of cybercrime, (2) online illicit marketplaces and the cryptomarkets, (3) the crypto-currency of cryptomarkets, (4) conundrum for law enforcement and postal authorities, (5) potential interventional strategies, (6) violence reduction, and (7) harm reduction. As noted earlier, this helped the researcher to view the research topic (cryptomarkets) from various criminological perspectives (i.e., illicit drug issue, drug policy and cybercrime) and identify an appropriate theoretical framework for this project. The literature review also assisted the researcher to identify a suitable research methodology.
2) *Theoretical Framework:* a number of theories have been adopted to analyse the activities of cryptomarkets. First, the illicit nature of online drug distribution has been conceptualised from the perspective of

cybercrime. This research mainly relied on the studies of Martin (2014) and Martin (2013) to conceptualise the activities of cryptomarkets through the realm of cybercrime. In addition, the researcher analysed cryptomarkets through the lens of discourse analysis. This is due to the fact that different groups (e.g., media, law enforcement agencies, and scholars) have different assumptions and use different language to describe cryptomarkets. Finally, in order to examine the implications associated with cryptomarkets, the researcher explored this new breed of drug market through current drug policy of Australia.

3) *Data Collection:* to obtain secondary data, various data archives that are hosted by Macquarie University were thoroughly searched. This process enabled the researcher to obtain numerous journal articles on cryptomarkets. There were several advantages associated with this process. It offered the opportunity for the researcher to save time and resources. The process of collecting secondary data also seemed to be ideal for this research, as the researcher had access to international and/or cross-historical data that may have been much more labour intensive to collect via traditional means. Secondary data collection provided the researcher with a 'tried-and-tested' set of data that has previously been collected and analysed by other researchers. According to Bryman (2008, p. 296), secondary data analysis is an ideal methodological approach for postgraduate students, as they have restricted word counts and a short amount of time. Another benefit of collecting secondary data is that students can obtain and report people's perspectives from all around the world. Hence, this methodology was the

most appropriate approach to answer the primary questions that were formulated for this research.

3.1.3 – Data Analysis

Since the study of cryptomarkets is a new area in criminology, the researcher selected exploratory research design for this project to analyse and reinterpret the collected data. This suggests that this project is an exploratory work. It is argued by Denscombe (2009) that exploratory research design is most appropriate to investigate topics with a limited body of theory. Taking that into account, an exploratory research design was selected for this project, as there is a limited body of theory on the illicit nature of cryptomarkets.

For this research project, the researcher examined and explored qualitative and quantitative data. In order to collect qualitative data on the illicit nature of cryptomarkets, the researcher mainly relied on the studies of Martin (2014; 2013), Barratt et al. (2014), Aldridge and Decary-Hetu (2014), and Van Hout and Bingham (2013; 2013a; 2013b). This research analysed and reinterpreted this qualitative data collected from the aforementioned studies. For quantitative data on cryptomarkets, the researcher obtained, analysed, and reinterpreted datasets from the studies of Barratt et al. (2013), Christin (2012) and Barratt (2012a).

Chapter 4: Analysis of Cryptomarkets through the Realm of Discourse Analysis

Language plays a crucial role when describing the illicit nature of cryptomarkets (Paul Gee, 2011; Schiffrin et al., 2001). There are often different types of languages used by commentators, law enforcement agencies, and academics when describing cryptomarkets. These languages differ significantly and also create different implications in society. In order to identify and examine those terminologies, it is crucial to conceptualise cryptomarkets through the realm of discourse analysis. The fourth chapter of this thesis is concerned with the language used by commentators, law enforcement officials and academics and how different language has different implications. First, this chapter briefly discusses how cryptomarkets can be analysed through the lens of discourse analysis. Furthermore, it identifies and analyses the language used by the commentators to describe this new breed of illicit drug market and how society perceives that language. Lastly, this chapter compares and contrasts the language and perceptions of law enforcement agencies and academics on online drug distribution. This is a significantly important chapter because commentators and law enforcement agencies often describe and cite cryptomarkets inaccurately.

4.1 – Discourse Analysis of Cryptomarkets

Discourse analysis is a modern discipline of the social science and it is an approach to study and analyse written, vocal, or sign language (Paul Gee, 2014; Paul Gee, 2011). Similarly, Schiffrin et al. (2001) also maintain that discourse analysis is a rapidly growing and evolving field. The study of discourse is the

study of language use (Schiffrin et al., 2001, p. 1). This indicates that discourse analysis focuses on specific instances of language since different language has different implications. In language, there are important connections among saying (informing), doing (action), and being (identity). People use different styles or varieties of language for different purposes. For instance, certain statements may sound positive; however, in reality, they may have negative consequences (Paul Gee, 2011). According to Paul Gee (2011), generally, language is used to make things significant or insignificant.

Taking that into account, it can be argued that language plays a pivotal role in society because a certain language could convey certain messages. This means that discourse analysis is a useful method that offers the opportunity for criminologists to identify and analyse the language that is being used by commentators, law enforcement agencies, and academics to describe this new breed of illicit drug trade. In other words, it is advantageous to conceptualise cryptomarkets through the realm of discourse analysis. This is due to the fact that there are numerous languages / terms used by different groups (i.e., media, law enforcement agencies and academics) to describe and analyse these illicit drug markets.

4.1.1 – Language Used by Commentators to Describe Cryptomarkets

The media has always played an important role in the construction of criminality and the criminal justice system (Dowler, 2003). The public's perception of criminals, victims, deviants and law enforcement officials is largely determined by their portrayal in the mass media. Research (Dowler, 2003; Surrette, 1998;

Roberts and Doob, 1990) demonstrates that the majority of public knowledge about crime and justice derived from the media. The portrayal of crime on television and printed media is significantly more violent, random and more dangerous than crime in the "real" world. This suggests that the mass media is often responsible in creating fear of crime among the general public. In addition, Surette (1998) claims that print and broadcast news regularly use persuasive language to personify the police as ineffective and incompetent.

According to Martin (2014), even in the case of cryptomarkets, commentators have repeatedly used misleading language when describing these illicit drug markets. For example, the mass media (Smith, 2014; Goldstein, 2013; Mansfield, 2013; Robinson, 2012) has often described this new breed of illicit drug market as "eBay for drugs". While this term may be used with positive intent (i.e., to inform and educate the public), it tends to have negative implications on several counts. First, it has the potential to create moral panic amongst communities. This is due to the fact that the term (i.e., eBay for drugs) itself indicates that cryptomarkets are a transformative innovation that enables people to distribute or obtain illicit goods via the Internet – with minimal technological skills (Phelps and Watt, 2014; Aldridge and Decary-Hetu, 2014; Van Hout and Bingham, 2013; Barratt et al., 2013; Van Hout and Bingham, 2013b).

Taking that into account, it can also be suggested that the term "eBay for drugs" may have been used to portray a negative image of the police. According to Paul Gee (2011), in some instances, certain statements may have a number of

meanings. Those statements are often used for multiple purposes. One of the potential implications of using such a term (eBay for drugs) is to create tension among the general public and law enforcement officials. Not only that, the term itself creates chaos and turmoil in society since it indicates a sign of weakness and failure on the part of law enforcement. This is due to the fact that law enforcement agencies are perceived as having some control (to a certain extent) over the traditional illicit drug trade. In spite of these modern and sophisticated computer technologies, law enforcement authorities have little or no control over these new and lucrative illicit drug markets (Martin, 2014; Aldridge and Decary-Hetu, 2014; Van Hout and Bingham, 2013; Barratt et al., 2013; Van Hout and Bingham, 2013b; Martin, 2013; Christin, 2012). Moreover, according to Paul Gee (2011), the news media is known for using emotive language to sell more media. This indicates that the news media used this term (eBay for drugs) to maintain market share while portraying a negative image of law enforcement agencies.

4.1.2 – Perspective of Law Enforcement Officials on Cryptomarkets

Law enforcement agencies have often seen and categorised this new breed of drug trade as a variant of conventional drug distribution rather than viewing and classifying the activities of these sites through the realm of cybercrime (Martin, 2014; Martin, 2013). Throughout history and also in the present day, drug dealers used traditional techniques (i.e., wholesaling, importing, street dealing) to distribute illicit drugs. There are a number of consequences (i.e., drug-related harm, drug-related death, and systemic drug-related violence) associated with those traditional drug-dealing techniques (United Nations Office on Drugs and

Crime, 2014; National Drug and Alcohol Research Centre, 2013; Caulkins and Reuter, 2009; Reuter, 2009; Moore, 2008; Blumstein, 1995). These factors are discussed in depth in the next chapter.

In this new era of global trade powered by modern and sophisticated computer technologies, vendors are able to anonymously advertise and distribute their illicit products to a worldwide market (Martin, 2014; Aldridge and Decary-Hetu, 2014; Van Hout and Bingham, 2013; Barratt et al., 2013; Van Hout and Bingham, 2013b; Martin, 2013; Christin, 2012). Contemporary research (Aldridge and Decary-Hetu, 2014; Van Hout and Bingham, 2013a; Martin, 2013) indicates that cryptomarkets differ significantly from conventional forms of drug distribution, as they tend to eliminate a number of factors typically associated with traditional form of drug dealing. Due to the "war on drugs" and the illicit nature of the cryptomarkets, law enforcement officials mainly focus on drug-related offences that are committed in these lucrative drug markets rather than analysing the foundation or core of the issue.

Policing authorities perceive that it is more of a drug-related issue than a computer-related issue and/or cybercrime (Martin, 2014; Martin, 2013). This perception raises numerous issues, complicates the situation and creates misconception in the general public. This is due to the fact that cryptomarkets not only distribute drugs, they also offer a wide range of other illicit goods and services (Christin, 2012). For example, through cryptomarkets individuals can acquire stolen items or information, stolen credit cards, stolen passports, personal information, counterfeit currency, and weapons of any kind (Christin,

2012, p. 3). Empirical research suggests that these illicit drug bazaars also offer contract killing (Martin, 2014; Christin, 2012). The argument provided by Martin (2014) and Christin (2012) suggests that law enforcement should not misinterpret the illicit nature of cryptomarkets as only a drug-related issue, because these illicit e-commerce sites specialise in a wide range of criminal activities. In order to analyse the illicit nature of cryptomarkets, law enforcement agencies should perceive the activities of cryptomarkets as a cyber-related issue. Interestingly, a number of studies (Martin, 2014; Barratt et al., 2014; Aldridge and Decary-Hetu, 2014; Martin, 2013) have analysed the activities of these illicit sites through the realm of cybercrime and proposed a new cybercrime concept called the cryptomarket. Martin (2014) argues that the rapid growth in communication technologies poses a significant challenge for academics and forces them to develop and establish new concepts and theories.

4.1.3 – Scholarly Perception of Cryptomarkets

A number of scholarly studies (Martin, 2014; Aldridge and Decary-Het, 2014; Barratt et al., 2014; Van Hout and Bingham, 2013; Martin, 2013; Barratt, et al., 2013; Van Hout and Bingham, 2013b; Christin, 2012; Barratt, 2012) have been published analysing different facets of cryptomarkets. There are studies (Van Hout and Bingham, 2013; Barratt, 2012) that refer to cryptomarkets as "eBay for drugs". While it may be a general description of cryptomarkets, it does not accurately describe the operations of these illicit sites (Aldridge and Decary-Het, 2014). This suggests that there is also a critical debate within the scholarly community (Martin, 2014; Aldridge and Decary-Het, 2014; Barratt et al., 2014; Martin, 2013; Van Hout and Bingham, 2013; Barratt, 2012) when describing

cryptomarkets and their operations and infrastructure. This is due to the fact that there are a number of studies (Phelps and Watt, 2014; Van Hout and Bingham, 2013; 2013a; 2013b; Barratt, 2012) that used inaccurate terminologies to describe the infrastructure of cryptomarkets. Van Hout and Bingham (2013, p. 1), for instance, claim that a cryptomarket is a platform that offers illicit goods and services and it operates on the "*Deep Web*". *Deep Web* is one of the divisions of the web that contains a massive number of collections that are mostly invisible to search engines (Wright, 2008; King, 2004, p. 7). Commonly, *Deep Web* collections consist of a database which is accessible only through a search interface (Wright, 2008; King, 2004). In short, deep web is a database that hosts a huge volume of crucial information which cannot be easily accessed by hyperlinks. Examples of deep web content are phone directories, subject directories, patent collections, book collections, news articles and holiday booking interfaces (Wright, 2008; King, 2004, p. 7). Van Hout and Bingham (2013) therefore argue that cryptomarkets also operate on the deep web, as these lucrative illicit drug markets are not searchable by standard search engines such as Google.

However, the studies of Aldridge and Decary-Het (2014), Martin (2014), Barratt et al. (2014) and Martin (2013) suggest that cryptomarkets do not operate on the deep web; in fact, they operate on the encrypted part of the Internet, often known as the *'dark net'*. According to Berthier and Cukier (2008), Bethencourt et al. (2007), and Bailey et al. (2006), the dark net refers to part of the Internet that cannot be found using Google or other regular search engines. It is inaccessible without a special software (e.g., TOR) product. Empirical evidence

(Berthier and Cukier, 2008; Bethencourt et al., 2007; Bailey et al., 2006) suggests that the dark net is sometimes confused with the deep web. The deep web is composed of academic resources maintained by universities, and contains nothing sinister whatsoever. And the dark net is the anonymous part of the Internet that allows its users to send encrypted data and conduct anonymous transactions. Hence, the studies of Martin (2014), Aldridge and Decary-Het (2014), Barratt et al. (2014) and Martin (2013) claim that cryptomarkets operate on the dark net. The rationale behind this argument appears to be that the operations of cryptomarkets are dependent upon the TOR network and an encrypted electronic currency (e.g., Bitcoin).

Taking that into consideration, it may be useful to refer to this new breed of illicit drug market as a dark net marketplace or *cryptomarket* (Martin, 2014, p. 2; Aldridge and Decary-Het, 2014; Barratt et al., 2014; Martin, 2013). Compared to the language used by the media and law enforcement agencies, the term cryptomarket seems to be more straightforward and well defined by scholars. Aldrige and Decary-Het (2014, p. 4) assert that:

> A cryptomarket employs from amongst a range of strategies to hide the identity of its participants and transactions, and the physical location of its services. These include: anonymisation services like TOR and I2P (anonymous service similar to TOR) that hide a computer's IP address when accessing the site; decentralised and relatively untraceable cryptocurrencies like bitcoin and litecoin for making payments; and encrypted communication between market participants via PGP (Pretty Good Privacy computer program).

When considering this definition in further depth, it becomes apparent that cryptomarkets do not distribute anything, rather they host the infrastructure or main platform for consumers and distributors to carry out transactions among

themselves (Martin, 2014). *"The role of a cryptomarket is therefore as a facilitator and broker rather than a direct participant in the illicit exchange"* (Martin, 2014, p. 3). These lucrative drug markets can be accessed by anyone who has an Internet-enabled computer and a bank account to purchase Bitcoins (Martin, 2014). Moreover, the aforementioned definition provided by Aldrige and Decary-Het (2014) suggests that this type of drug distribution differs significantly from conventional forms of drug dealing. It is deduced by Aldrige and Decary-Het (2014) that the novelty nature of cryptomarkets forced law enforcement agencies around the world to change their traditional policing techniques when dealing with and/or targeting these sites. This implies that law enforcement agencies should shift their focus towards conceptualising and analysing the activities of cryptomarkets through the realm of cybercrime, as these illicit drug bazaars are facilitated by modern and sophisticated computer technologies.

4.1.4 – Conclusion

This chapter has analysed cryptomarkets through discourse analysis theory. To conclude, there are different terminologies used by media, law enforcement agencies and academics when describing this novel form of drug distribution. It is evident that the terminology (i.e., eBay for drugs) used by the mass media has several negative implications. This indicates that media play an active role in creating tension in society, as they often use persuasive language to send indirect messages to communities and personify the police as ineffective. Furthermore, it is increasingly apparent that law enforcement agencies hold two distinct perceptions when describing and analysing the activities of

cryptomarkets. In order to draw a distinct line between online drug distribution and conventional form of drug dealing, law enforcement agencies need to shift their focus towards the facilitator (i.e., cryptomarket) of this lucrative illicit drug trade. Immediately, after shifting their focus, law enforcement agencies would reach a conclusion that this novel form of illicit exchange is not only a drug-related issue, it is also cyber-related issue.

Chapter 5: Analysis of Cryptomarkets

The development of anonymous networks (i.e., TOR Network) has facilitated cryptomarkets. This new breed of online illicit market has changed the nature of drug distribution and challenged law enforcement agencies (Martin, 2014; Aldridge and Decary-Hetu, 2014; Van Hout and Bingham, 2013, Martin, 2013; Van Hout and Bingham, 2013b; Barratt et al., 2013; Christin, 2012). Due to the illicit nature of cryptomarkets, policing authorities want to disrupt and target online drug sites (Aldride and Decary-Hetu, 2014). The following chapter discusses the characteristics of cryptomarkets and the current drug policy of Australia and why it is not expedient for law enforcement agencies to disrupt or target online drug sites under the existing policy. Firstly, it analyses how cryptomarkets reinforce certain aspects of the current Australian drug policy and how they may in fact assist the Australian Government, the Australian Institute of Health and Welfare and drug-users. In addition, it scrutinises how cryptomarkets contribute positively in reducing harm, drug-related mortalities and most profoundly systemic drug-related violence.

5.1 – The Impact of Cryptomarkets on Contemporary Society

The advancement in computer technologies, in particular the Internet, and the shift towards widespread global availability of illicit goods have opened new avenues for drug distributors and consumers. Today, drugs can simply be purchased and/or distributed online. This type of drug distribution varies significantly from the traditional type of drug dealing since cryptomarkets operate on the "dark net". As mentioned in the previous chapter, cryptomarkets are often described by media (Smith, 2014; Goldstein, 2013; Mansfield, 2013;

Robinson, 2012) as "eBay for drugs" that allow drug dealers to anonymously advertise and sell their goods to a global market and to a great extent out of reach of law enforcement. Policing authorities, therefore, have a strong interest in disrupting and targeting cryptomarkets. Here, the primary question that needs to be addressed is "Should law enforcement agencies disrupt or target cryptomarkets?" Due to the illegal nature of the cryptomarkets, it seems logical for law enforcement agencies to disrupt or target these new breeds of illicit drug markets, as it is their responsibility and duty to maintain law and order and minimise illicit activities.

However, before taking any action, it is crucial for law enforcement agencies to analyse and explore every facet of cryptomarkets – as there are substantial reasons suggesting that law enforcement agencies should not disrupt or target them. For example, it is deduced by Van Hout and Bingham (2013, p. 1) that *"online public drug sites provide user information on outcomes, experiences, popularity, availability and sourcing mechanism, optimum use and harm reduction practices".* This new type of online drug market and drug distribution also offers individuals the opportunity to be relatively free from the violence typically associated with traditional drug markets (i.e., organised drug dealings) (Martin, 2014; Aldridge and Decary-Hetu, 2014; Barratt et al., 2013; Van Hout and Bingham, 2013; Christin, 2012).

5.1.1 – Harm Reduction through Cryptomarkets and Online Forums

Cryptomarkets have numerous valuable structural features that enable anonymous discussion and sharing of information. Buyers and sellers frequently

and anonymously publish drug-related information in public forums. Prior to the emergence of this new breed of online drug retail, drug dealers and consumers did not have such a tool to extensively share their personal experiences with other drug-users. The main sources of information drug-users previously relied upon were the government interventional and educational programs, personal experiences and advice from other drug-users (Moore, 2008). Drug-users are currently able to publish their personal narratives on the Internet (e.g., chat forums) to instruct other drug-users on how to use drugs more safely and how to avoid unpleasant experiences with drugs (Barratt et al., 2013). It is increasingly apparent that this sort of information cannot be obtained elsewhere, where drug-users share their personal drug experiences to educate and exercise harm reduction amongst each other. Through online public forums, moderators, administrators and users work in partnerships and groups to minimise the risk of harm associated with drugs (Barratt et al., 2013; Van Hout and Bingham, 2013; Barratt, 2012).

Interestingly, Barratt (2012a) conducted an online survey with drug-users, moderators and administrators from 40 different Internet chat forums where drugs were discussed in Australia. In this survey, participants were asked what they are striving to achieve when participating in public forums. A vast majority of the respondents (88%) indicated that they participate in public forums for the purpose of harm reduction (Barratt et al., 2013). The figure provided by Barratt et al. (2013) also indicates that cryptomarkets may play a central role in reducing drug-related fatalities by preventing individuals from drug overdose amongst those who purchase drugs via cryptomarkets. Drug overdose is a

serious and concerning global issue. It is responsible for thousands of deaths each year. *"An estimated 183,000 (range: 95,000-226,000) drug-related deaths were reported in 2012"* (United Nations Office on Drugs and Crime, 2014, p. xi). According to the United Nations Office on Drugs and Crime (2014) and Australian Medical Association (2013), Australia has a higher than average drug mortality rate and it is rising steadily. Despite the fact that the Australian Government devotes millions of dollars to harm reduction programs (National Drug and Alcohol Research Centre, 2013), at least three Australians die each day as a direct consequence of drug overdose. According to the Australian Bureau of Statistics (2005), illicit drug overdose claimed 8,691 Australian lives between 1997 and 2005. It claimed an average of 1,086 Australian lives each year and almost 3 individuals each day. Taking that into account, it can simply be argued that disrupting and targeting cryptomarkets does not seem to be expedient for the Australian Government/public. While the proportion of drug-users who obtain *detailed* drug-related instructions and purchase drugs through cryptomarkets is relatively low compared to those drug-users who acquire drugs from traditional street drug distributors, it can be argued that disrupting and/or targeting cryptomarkets would further jeopardise the situation and may increase the number of drug-related mortalities and drug abuse in Australia.

It is worth noting that while disrupting or targeting cryptomarkets would prevent individuals from conducting online illicit transactions, it may not prevent them from obtaining and distributing illicit goods through traditional illicit drug marketplaces (Martin, 2014; 2013). The argument provided by Martin (2014; 2013) indicates that targeting cryptomarkets would not reduce the number of

drug-users in Australia because traditional drug distribution would take place. This would further complicate the situation for the Australian Government, Australian Institute of Health and Welfare and Australian public, as individuals may have limited access to detailed drug-related information and there would be more cases of drug-related deaths and drug abuse. Thus, it may be beneficial for governments around the world to encourage and increase the proportion of users on cryptomarkets to reduce and/or minimise drug-related mortalities and drug abuse.

It therefore seems reasonable to assume that cryptomarkets contribute in reducing the number of drug-related mortalities by encouraging users to both produce and consume drug-related information and also discourage potentially harmful dissemination of information (Van Hout and Bingham, 2013; Barratt et al., 2013). This may suggest that while the primary aim of people using these sites is to distribute illicit drugs on a global scale, they also assist governments, in particular the Australian Government, the Australian Institute of Health and Welfare and Australian educational institutions. One of the reasons that cryptomarkets assisted the Australian Government is the fact that for last three decades, the government adopted and imposed a policy of harm reduction (Trinmingham, 2012).

5.1.2 – The Link between Australian Drug Policy and Cryptomarkets

The current drug policy of Australia emphasises that a drug-free society is unachievable. However, reducing drug-related harm seems feasible by reconsidering and establishing new approaches (Nossal et al., 2012;

Trimingham, 2012). Through the existing illicit drug policy, the Australian Government works towards:

1. Increasing knowledge and understanding of drug use and issues in the community.
2. Increasing the likelihood that people who currently use or have used drugs can lead a normal and useful life as full members of the community.
3. Minimising deaths, disease, crime and corruption arising from drug use.
4. Ensuring that a wide range of attractive, easy to use, safe and affordable health and social interventions are available for those concerned by their drug use, including evidence-based drug treatment which are properly resourced and are of the same high quality as other parts of the health care system. (Trimingham, 2012)

Under current drug policy, the Australian federal and state governments spend 1.7 billion dollars on drug management each year (National Drug and Alcohol Research Centre, 2013). Two thirds of the total drug budget (66% or $1.12 billion) is spent on law enforcement. Just over 21% or $361 million is devoted towards treatment. Just 9% or $157 million is spent on drug prevention. Strikingly, only 2% ($36 million) of the total budge is spent on harm reduction (National Drug and Alcohol Research Centre, 2013). While this is a substantial sum, it is undoubtedly a tiny proportion of the overall drug budget. This suggests that in spite of adopting harm reduction drug policy, the Australian

federal and state governments do not devote a substantial amount of money on harm reduction, compared to spending hundreds of millions of dollars on law enforcement. As a matter of fact, the Australian Government has significantly reduced funding for harm reduction (National Drug and Alcohol Research Centre, 2013). According to Moore (2008), the Australian Government deducted $8.8 million from a total of $44.8 million that was previously spent on harm reduction. This implies that the drop in spending on harm reduction is a concerning issue for drug-users and health professionals. This is because there would be very limited government resources to instruct or advise drug-users on how to minimise harm and avoid bad experiences while consuming drugs.

Significantly, it is worth noting that cryptomarkets reflect and reinforce certain aspects of the current Australian drug policy, in particular those aforementioned aims and they should not be disrupted or targeted under the existing policy. In order to interrupt online drug markets, the Australian Government and policing authorities need to reconsider the current drug policy and/or adopt new and effective drug policies. This is due to the fact that there is no specific reference to cryptomarkets in the current Australian drug policy.

Furthermore, as mentioned previously, the Australia Government devotes only 2% of the total drug budget of 1.7 billion dollars on harm reduction. Due to limited resources, money and capacity, a very low proportion of drug-users can access and receive information on how to reduce drug-related harm (National Drug and Alcohol Research Centre, 2013; Moore, 2008). A number of those drug-users who are eligible to access and receive information, sense discomfort

participating in these government funded harm reduction and educational programs (Moore, 2008). The primary reason that they sense discomfort to participate is the fact that their drug identities are secret. Their families and friends may not be aware of their drug issues (Moore, 2008). Thus, they hesitate to take part in government funded educational and harm reduction programs.

In contrast to government intervention and harm reduction programs, individuals tend to feel confident participating in online public forums, since they do not reveal their true identities (Martin, 2014; Aldridge and Decary-Hetu, 2014; Van Hout and Bingham, 2013, Martin, 2013; Van Hout and Bingham, 2013b; Christin, 2012). It is argued by Van Hout and Bingham (2013) that individuals who engage in online drug sites maintain their "non drug identities" by keeping their "drug identities" undisclosed and private. They believe that *"drug use is for a personal journey, and not something to be shared with others"* (Van Hout and Bingham, 2013, p. 5). This may perhaps mean that drug-users do not sense any discomfort when participating in online public forums because they believe that online drug sites are the only trusted places to obtain comprehensive and reliable information on drugs (Barratt et al., 2013; Van Hout and Bingham, 2013).

Disrupting and targeting online drug sites would potentially create further, significant challenges for the Australian Government and law enforcement agencies. First, drug-related discussion would likely shift to "corporate-controlled walled gardens" (e.g., Facebook) (Barratt et al., 2013, p. 2). In other words, individuals may use social media and other communication and mobile

devices to discuss and share drug-related information. In this case, governments and law enforcement agencies may continue to have limited or no control over preventing individuals from discussing and sharing drug-related information. In addition, organised drug distributors would adopt the traditional form of drug dealing (i.e., street dealers and organised drug trafficking) (Aldridge and Decary-Hetu, 2014). This would further complicate the situation, and other drug-related issues (i.e., systemic violence) may arise.

5.1.3 – Violence Reduction through Cryptomarkets.

Disruption of cryptomarkets may increase systemic violence amongst organised crime groups. The use of violence amongst organised crime groups would simply be for maintaining revenues and other drug-related activities. Violence is traditionally used amongst organised crime groups to control market share, resolve conflicts and protect territories (Reuter, 2009; Caulkins and Reuter, 2009; Blumstein, 1995). Gangs and/or organised crime groups that derive their primary financing from illicit drugs have been incriminated in a significant number of assaults and homicides (Werb et al., 2011; Agren, 2010; Castle, 2009; Decker, 2003; Hutson et al., 1995). This suggests that most of this gang-related violence (i.e., drive-by shootings, homicides, gun crimes) may possibly be the result of the expansion of drug gangs in Sydney, Australia. In order to avoid issues associated with drugs such as drug-related harm, mortalities and systemic drug-related violence, law enforcement authorities should not interrupt cryptomarkets. The realm of this new breed of drug market enables vendors to effectively exchange goods with many fewer risks typically associated with the conventional form of drug exchange (Aldridge and Decary-Hetu, 2014; Van

Hout and Bingham, 2013, Martin, 2013; Van Hout and Bingham, 2013b; Christin, 2012). Examples of risks that are typically associated with the conventional form of drug exchange include violence, intimidation and territorialism (Reuter, 2009; Bouchard, 2007; Bouchard and Tremblay, 2005; Levitt and Venkatesh, 2000; Reuter and Kleiman, 1986).

Recently, Sydney has experienced increased gang/drug-related violence (Birdsey, 2012). According to recent reports published by New South Wales Bureau of Crime Statistics and Research, most of those drive-by shootings and gun crimes are directly linked with the distribution of illicit drugs (Birdsey, 2012). Currently, organised crime groups such as outlaw motorcycle gangs are fighting over drugs and territories to gain and maintain market share (Birdsey, 2012). While there are no scholarly studies that analysed systemic drug-related violence in Australia, it is deduced by Sutton (2013) that Australia is seeing a significant increase in violence directly related to illicit drugs. Organised crime groups create mayhem in every Australian state and territory to protect turfs, distribute more drugs and gain market share. Outlaw motorcycle gangs are major competitors in Australia's drug trade who bring their violent disputes into public spaces and carry out "brazen shootings" (Sutton, 2013). This drug-related violence and/or wars among organised crime groups are putting innocent lives at growing risk of getting caught up in the crossfire.

Systemic drug-related violence is a less significant issue in Australia when compared to drug-related violence in Mexico. It is estimated that over the past seven years, tens of thousands of people have been killed due to systemic drug-

related violence (BBC News, 2014). It is, therefore, claimed by Johnson et al. (2000), Romero-Daza et al. (2003), Ousey and Lee (2004), Martin et al. (2009) and Werb et al. (2011) that systemic drug violence is amongst the primary concerns of communities around the world. While systemic drug-related violence claims a considerable number of lives each year, it is immensely difficult to obtain an accurate global figure on how many innocent lives are lost due to systemic drug violence. Violence associated with illicit drugs is considered to be very common in urban areas (Johnson et al., 2000; Romero-Daza et al., 2003; Ousey and Lee, 2004; Martin et al., 2009; Werb et al., 2011). This is due to the fact that traditional drug distributors mainly use violence to settle disputes and/or conflicts with other rival gangs, dominate illicit drug markets and increase their market share.

In contrast, violence is very less likely to erupt among vendors of cryptomarkets since they use highly sophisticated computer technologies to remain anonymous. They are also geographically distant and they never meet face-to-face (Martin, 2014; Van Hout and Bingham, 2013; Martin, 2013; Van Hout and Bingham, 2013b). In addition, online drug distributors compete with one another using non-violent methods to gain and maintain market share; they are less likely to encourage any type of activities that initiate violence. In order to compete and gain more market share of the lucrative illicit drug trade, online drug distributors employ special and distinctive types of skills. For example, in the realm of cryptomarkets, having good writing skills, a good reputation as well as providing good customer service is more important than having fighting skills (Martin, 2014; Aldridge and Decary-Hetu, 2014; Van Hout and Bingham, 2013,

Martin, 2013; Van Hout and Bingham, 2013b). This suggests that the new breed of drug dealing offers distributors and consumers the significant benefit of avoiding the risk of street violence and also creating distance among them (Martin, 2014; Van Hout and Bingham, 2013; Martin, 2013; Van Hout and Bingham, 2013). It is, therefore, important to note that online drug distributors are less harmful than traditional 'street' based drug distributors.

According to Aldridge and Decary-Hetu (2014), online drug distributors tend to be more educated than those average street drug dealers and hence they discourage any type of activities that initiate violence. This suggests that while both traditional and online drug distributors share similar ambitions (i.e., distributing drugs and maintaining revenue), their methods and cultural expectations for violence tend to be very different. Traditional drug distributors, for instance use force and violence to dominate market share of the lucrative illicit drug trade, while online drug distributors discourage and eliminate the likelihood of systemic drug-related violence. To dominate the illicit drug market, online drug distributors use competitive methods such as Halloween and Christmas discount specials, friendly and high standard customer service, assurance of quality products, and providing refunds on intercepted drugs (Aldridge and Decary-Hetu, 2014; Van Hout and Bingham, 2013; Martin, 2013; Van Hout and Bingham, 2013b; Christin, 2012). Disrupting and targeting may increase the risk of systemic drug-related violence such as gun crime, drive-by shootings, turf wars and homicides. Taking into consideration all the advantages and disadvantages of online drug distribution, policing authorities should consider every aspect of online drug sites before taking any action.

5.1.4 – Conclusion

This chapter has examined and explored various facets of cryptomarkets and how they differ from traditional form of drug distribution. Considering all the empirical evidence, it can simply be argued that cryptomarkets should not be targeted and disrupted under the current Australian drug policy. This is because there is no specific reference to cryptomarkets in the current Australian drug policy. Moreover, cryptomarkets assist the current drug policy of Australia since they contribute positively in reducing harm, drug-related mortalities and systemic drug violence. This implies that disrupting cryptomarkets would create further and significant challenges for law enforcement agencies. In order to disrupt and target cryptomarkets, the Australian law enforcement agencies need to propose a new and advanced drug policy.

Chapter 6: Targeting Cryptomarkets

Law enforcement agencies are closely monitoring the activities of cryptomarkets to collect digital evidence against the actors (buyers, sellers and administrators) of these illicit drug markets (Martin, 2014; Aldridge and Decary-Hetu, 2014; Van Hout and Bingham, 2013, Martin, 2013; Van Hout and Bingham, 2013b; Barratt et al., 2013; Christin, 2012). According to the Australian Federal Police (AFP) (2012), individuals engaging in illicit activities through cryptomarkets will not always remain anonymous. Customs, Border Protection and other partner agencies are therefore committed to target these illicit drug bazaars (Australian Federal Police, 2012). This chapter analyses the current intervention strategies that are identified to target and disrupt the activities of cryptomarkets. First, it identifies how many intervention strategies are available to target cryptomarkets and how effective those strategies may be. Furthermore, the following chapter offers an alternative solution that may assist governments around the world.

6.1 – Potential Interventional Strategies

As noted earlier, due to the illicit nature of the goods distributed on cryptomarkets, it is increasingly apparent that law enforcement agencies have a strong interest in targeting these markets (Christin, 2012). To date, they have had little success in disrupting the operations of cryptomarkets and reducing the overall number of buyers and sellers. In fact, the overall number of buyers and sellers is rapidly growing (Martin, 2014; Aldridge and Decary-Hetu, 2014; Van Hout and Bingham, 2013; Martin, 2013; Van Hout and Bingham, 2013b; Barratt et al., 2013; Christin, 2012). It is claimed by Martin (2013) that the rapid growth

of buyers and sellers in cryptomarkets suggests that law enforcement is largely failing. This also means that the complex nature and novelty of online drug distribution has significantly challenged law enforcement agencies around the world. Governments and drug enforcement agencies are therefore struggling to put an end to cryptomarkets (Martin, 2014; Aldridge and Decary-Hetu, 2014; Van Hout and Bingham, 2013; Martin, 2013; Van Hout and Bingham, 2013b; Barratt et al., 2013; Christin, 2012).

Nevertheless, it is important to explore and examine what strategies are currently available to prevent people from buying and selling illicit goods/drugs through cryptomarkets and how effective those strategies are. Barratt et al. (2014), Martin (2014), Barratt et al. (2013), and Christin (2012) have identified a wide range of interventional strategies that may disrupt the operations of cryptomarkets and also reduce the number of buyers and sellers. Those four potential interventional strategies are (1) disrupting the TOR network, (2) disrupting the financial infrastructure, (3) disrupting the delivery model, and (4) undercover investigation (Martin, 2014; Barratt et al., 2014, p. 784; Christin, 2012, p. 21).

6.1.1 – Disrupting the TOR Network

The first possible intervention strategy for law enforcement is to disrupt the TOR network. TOR is one of the two fundamental pillars of the cryptomarkets (Martin, 2014; Aldridge and Decary-Hetu, 2014; Van Hout and Bingham, 2013; Barratt et al., 2013; Martin, 2013; Christin, 2012). This means that cryptomarkets cannot operate without TOR. In order to target cryptomarkets, it

seems logical to disrupt the TOR network. However, when exploring this strategy in further depth, it appears to be significantly difficult to put it in practice. Christin (2012) claims the rationale behind this argument appears to be that cryptomarkets represent a very small proportion of the overall TOR traffic. Disrupting the TOR network for the purpose of targeting cryptomarkets would create further issues for governments around the world (Christin, 2012). There are numerous beneficial features associated with the TOR network. For instance, a considerable number of vulnerable and oppressed individuals regularly use TOR to communicate without fear of reprisal (Christin, 2012; Barratt, 2012). Since the TOR network has numerous beneficial features, it would come with a significant cost for law enforcement agencies to disrupt the entire TOR network.

Moreover, there are other methods that can simply be embraced and/or implemented to roughly estimate the location of an individual who is using a hidden service of TOR to conduct some sort of illegal activities (Overlier and Syverson, 2006; Murdoch, 2006). This suggests that there are weaknesses in TOR that can be exploited without dismantling the entire network. Overlier, and Syverson (2006), for instance, argue that timing and intersection attacks could be used to locate hidden services of TOR. Similarly, Murdoch (2006) asserts that the clock skew method could be used to roughly estimate the location of a hidden service. However, this strategy tends to be complicated and challenging for governments and law enforcement agencies. Just by implementing this strategy, governments are required to spend a substantial amount of money to educate and train their law enforcement agents on how to locate hidden services of TOR. In addition, even if law enforcement agencies target the entire TOR

network, there are other alternative networks similar to TOR such as Cloudnymous, CyberGhost VPN, Hotspot Shield, etc. This indicates that targeting the TOR network would be ineffective, time consuming and would not minimise the population of buyers and sellers on cryptomarkets (Barratt et al., 2013; Martin, 2013; Van Hout and Bingham, 2013; Christin, 2012). This would perhaps mean that law enforcement agencies should consider embracing other intervention strategies.

6.1.2 – Disrupting the Financial Infrastructure

The second possible intervention strategy is to attack the financial infrastructure supporting cryptomarkets. The realm of this new breed of drug markets is largely dependent upon an encrypted electronic currency called Bitcoin (Barnet, 2014; Barratt et al., 2014; Martin, 2013; Van Hout and Bingham, 2013). It is claimed by Christin (2012) that Bitcoin is an extremely volatile currency. This is due to the fact that the value of Bitcoin has fluctuated wildly on numerous occasions. For example, in June 2011 a large number of Bitcoins was stolen from the Mt. Gox exchange. This created chaos amongst users of Bitcoin and also caused an abrupt collapse of the currency. According to Christin (2012), law enforcement agencies could also pursue this strategy to manipulate the currency to create instabilities and delay transactions. Taking that into consideration, in May of 2013, U.S. authorities seized the assets of Mt. Gox, one of the world's largest Bitcoin exchanges at the time (Kien-Meng Ly, 2014). The incentive behind this seizure was due to the fact that Mt. Gox was engaging in the business of money transmission without an appropriate license. Consequently, this seizure forced Mt. Gox to file for bankruptcy and shut down

its website on February 28, 2014, after losing approximately 750,000 of its customers (Kien-Meng Ly, 2014).

Despite the fact that policing authorities impelled Mt. Gox to shut down, it did not have a significant impact in reducing number of sales and distributions of illicit goods on cryptomarkets. As a matter of fact, sales on Silk Road 1.0 (one of the major cryptomarkets) increased from an estimated $14.4 million in mid 2012 to $89.7 million by the end of 2013 (Aldridge and Decary-Hetu, 2014). The figure provided by Aldridge and Decary-Hetu (2014) suggests that there was a more than 600% increase in the course of 15 months. This would perhaps mean that by targeting Mt. Gox, law enforcement agencies may have temporarily disrupted the activities of cryptomarkets. This is because there are other alternative crypto-currencies (i.e., Stellar, Litecoin, Peercoin, Dogecoin etc.) that allow individuals to conduct online transactions (Ren, 2014). Taking that into account, it can be argued that disrupting the financial infrastructure would not prevent individuals from buying and distributing illicit drugs on the Internet. Hence, law enforcement agencies should implement more effective, reliable and cost-efficient strategies to reduce the number of sales and distributions of illicit goods.

6.1.3 – Disrupting the Delivery Model

Another potential intervention strategy is to disrupt the delivery model (Barratt, 2012). One of the scholarly arguments is that in order to disrupt the activities of cryptomarkets, law enforcement agencies should strengthen their border protection tactics at the post office and/or at customs to prevent illicit goods

being delivered to their desired destination (Christin, 2012). At the end of each transaction conducted via a cryptomarket, a seller needs to physically dispatch goods to a nominated address. Through postal delivery, vendors can simply distribute illicit goods to a worldwide market of customers (Martin, 2014; Aldridge and Decary-Hetu 2014; Barratt et al., 2013; Martin, 2013; Van Hout and Bingham, 2013; Barratt, 2012). Interestingly, a significant proportion of vendors seem not to worry about seizure because most items are labeled as shipping internationally, which suggests that the possibility of package loss or destruction is viewed as minimal by vendors (Christin, 2012). In order to prevent attracting the attention of custom and postal authorities, buyers are increasingly encourage to avoid purchasing drugs from countries with a reputation for exporting illicit drugs (i.e., Mexico, Colombia, Netherlands) (Martin, 2014; Martin, 2013). This offers law enforcement agencies, particularly postal and custom authorities, the opportunity to intercept and seize the illicit goods and may also lead to the arrest of the would-be importer (Barratt, 2012). Custom and postal authorities are therefore continuously pressured to thoroughly inspect postal items, in particular those items that arouse high degrees of suspicion (Martin, 2013, p. 8).

Nevertheless, there are also problems associated with this strategy. Firstly, online drug distributors use highly sophisticated concealment techniques to avoid attracting the attention of postal and custom authorities (Martin, 2014; Van Hout and Bingham, 2013; Martin, 2013; Barratt et al., 2013). This means that without a thorough inspection, it would be significantly difficult for postal and custom agents to identify the illicit packages amongst other legitimate

bundles of mail. In addition, Martin (2013, p. 8) claims that *"the rapidly expanding volume of global trade means that significantly more items are travelling through the international post than ever before*". In Australia, for instance, 16.5 million items are being delivered each day (Australia Post, 2013). This implies that it would be virtually impossible for Australian customs to thoroughly examine each of these items. According to Martin (2013, p. 8), detecting a small quantity of illicit drugs in this huge volume of mail is like locating a "needle among the haystack". One may argue that due to the large number of passengers passing through airports, and the large number of parcels arriving through couriers, it is also an issue for law enforcement agencies when policing traditional drug trade.

Although this is an issue when policing both traditional and online illicit drug markets, it is a more significant issue for law enforcement and postal authorities when policing cryptomarkets, as distributors of these illicit drug markets tend to import a very small amount of illicit goods through a very large volume of international posts. This would suggest that the rapidly expanding volume of mail also poses a significant challenge for the Australia Post, as they (Australia Post) have limited resources that prevent them from effectively and rigorously scanning domestic packages (Ormsby, 2012). Christin (2012, p. 22) argues that even with these limited resources and technical issues, when postal or custom authorities detect illicit packages, they are more likely to be destroyed, or returned to the sender. It is therefore worth noting that in order to be successful and increase the interception rate, governments would be required to (1) provide additional and advanced resources for Customs and other law enforcement

agencies, (2) introduce new laws that would allow postal and Custom authorities to interfere, detect and seize illicit postal items, and (3) employ and efficiently train more postal and Customs officers to protect national borders.

6.1.4 – Undercover Investigation

The fourth possible intervention strategy is to conduct undercover investigations (Barratt et al., 2014). Undercover investigations have proven to be the most successful strategy to disrupt and/or target cryptomarkets. It is claimed by Barratt et al. (2014) that in order to target and/or disrupt cryptomarkets, law enforcement agencies should consider embracing traditional police techniques. This would mean that undercover agents should pose as potential vendors or buyers to gather concrete evidence against the major actors of cryptomarkets. For example, recently, an undercover agent posed as a seller of drugs on the Silk Road 1.0 website to apprehend the alleged mastermind behind this notorious online drug market (Martin, 2014; Barratt et al., 2014; Goldstein, 2014). This eventually led the Federal Bureau of Investigation (FBI) to shut down Silk Road 1.0 (Kien-Meng Ly 2014). By October 2013, the FBI seized more than 33.6 million US dollars worth of Bitcoins and also arrested the alleged owner of the website, Ross Ulbricht, on charges of computer hacking conspiracy, narcotics conspiracy and money laundering conspiracy in connection with the operation of the Silk Road 1.0 website (Phelps and Watt, 2014; Kien-Meng Ly, 2014).

While the undercover investigation led the FBI to shut down Silk Road 1.0 and arrest the alleged owner of the website, it can simply be argued that this intervention strategy had little (short-term) impact in preventing individuals

from buying and selling illicit drugs through cryptomarkets, in particular the Silk Road 2.0 website.[1] This is because barely a month after the closure of the original site (Silk Road 1.0), the second version (Silk Road 2.0) was back in operation and the number of sales and distributions of illicit goods was rapidly increasing again (Martin, 2014; Aldridge and Decary-Hetu 2014; Barratt et al., 2014; National Drug and Alcohol Research Centre, 2014; Van Hout and Bingham, 2013; Martin, 2013). Thus, it is crucial to note that this strategy is problematic on several counts.

First, law enforcement agencies devote substantial amounts of money and time (i.e., two and half years in the case of Silk Road 1.0) to collect concrete evidence and apprehend the masterminds behind these markets. In some instances, whilst policing authorities executing this strategy (undercover investigation), a string of cryptomarkets may permanently terminate their services – as they may considered to be a threat for themselves (Martin, 2014). This suggests that in order to avoid being caught by law enforcement agencies, some actors of cryptomarkets tend to use temporary websites to distribute illicit goods. According to Martin (2014, p. 64), in the process of undercover investigation, a number of cryptomarkets may shut down due to security flaws, disturbance (hacking and looting) by external parties, and defrauding consumers and vendors. Also the closure of the Silk Road 1.0 website created fear amongst other administrators of cryptomarkets. This meant that due to the closure of the Silk Road 1.0 website, a number of other cryptomarkets terminated their services and shut down their sites. Although this may indicate a sign of victory

[1] During the submission process of this research, the Silk Road 2.0 website was shut down by law enforcement agencies (Wakefield, 2014).

for law enforcement agencies, in reality it poses a significant challenge for cyber investigators to obtain and analyse digital evidence and wrap up their investigation (Martin, 2014). This implies that undercover investigation is considered to be problematic, as it has little or no impact in preventing the rapid proliferation of buyers and sellers populating cryptomarkets and also requires large amounts of money and time to implement this strategy.

In addition, the history of undercover investigations has shown that despite law enforcement agencies routinely targeting cryptomarkets, it is becoming increasingly difficult for them to prevent the rapid emergence of new and advanced cryptomarkets (Martin, 2014; Aldridge and Decary-Hetu, 2014). According to Martin (2014, p. 65), *"each cryptomarket closure represents an opportunity for new sites to establish themselves and capture an unclaimed proportion of illicit market share and profit".* With the emergence of these new cryptomarkets, it is increasingly apparent that targeting online drug sites tends to be more of a problem than a solution. This is due to the fact that undercover investigation has had temporary impact in reducing the number of buyers and sellers on cryptomarkets. This would also mean that the actors in these markets are extremely conscious about the ramifications of this strategy (undercover investigation) and thus take precautionary measures while conducting illicit transactions over the Internet (Van Buskirk et al., 2013).

6.1.5 – Laissez-faire

Based on empirical evidence, a last possible alternative is actually not to interfere at all. This may sound controversial, since it indicates a sign of

weakness (Martin, 2014; Aldridge and Decary-Hetu 2014; Barratt et al., 2013; Martin, 2013; Van Hout and Bingham, 2013; Barratt, 2012; Christin, 2012). This is due partly to the fact that governments and law enforcement agencies have fought numerous battles and spent tens of billions of dollars in the war on drugs to minimise (1) drug cultivation, (2) drug importation (3) drug distribution and (4) the population of drug-users (Nossal et al., 2012; Trimingham, 2012). There are, however, studies that argue that reducing drug-related harm is feasible and considered to be more cost-efficient than enforcing drug prohibition (Nossal et al., 2012; Trimingham, 2012; Christin, 2012). As noted in the previous chapter, these highly sophisticated drug markets reduce drug-related harm, mortality rates and systemic drug violence. Thus, it can be claimed that taking down cryptomarkets would come at a high collateral cost. Currently, embracing this alternative (Laissez-faire) may perhaps sound unconventional; however, from an economics standpoint, it may become more attractive in the near future (Christin, 2012).

6.1.6 – Conclusion

This chapter has identified and analysed the current intervention strategies that can be embraced by law enforcement agencies to target and disrupt activities of cryptomarkets. By exploring and analysing all the empirical facts and figures, it is evident that law enforcement agencies have had little or no success in targeting and disrupting the activities of cryptomarkets. One of the reasons for this is that targeting cryptomarkets requires large amounts of money and time and it is considered to be ineffective. As well, targeting cryptomarkets is highly likely to have short-term impact in preventing individuals from buying and

selling illicit drugs through the Internet. This perhaps mean that individuals search for other means to effectively and anonymously distribute and obtain illicit drugs over the Internet. Furthermore, although policing authorities along with their partner agencies are actively working to put an end to these lucrative illicit drug markets, it is becoming increasingly difficult for them to prevent the rapid emergence of new and advanced cryptomarkets.

Chapter 7: Unintended Side Effects of Targeting Cryptomarkets

Cryptomarkets are changing the nature of drug distribution. Law enforcement agencies have strong interest to target and minimise the activities of cryptomarkets. Contemporary research (Martin, 2014; Aldridge and Decary-Hetu, 2014) indicates that, since the establishment of cryptomarkets, law enforcement authorities have disrupted and targeted a number of (i.e., Silk Road 1.0 and Utopia) these lucrative illicit drug markets. Despite the fact that law enforcement agencies targeted these sites, it did not have a long-term impact in minimising the activities of online illicit drug markets. As a matter of fact, the number of sales and distribution of illicit goods on cryptomarkets increased. This is due to the fact that the number of cryptomarkets is rapidly increasing and vendors maintain pages across multiple sites to gain market share (Benson, 2014). This suggests that targeting cryptomarkets would not prevent individuals from obtaining and distributing illicit goods online and there are numerous unintended side effects when disrupting and targeting these illicit drug bazaars. This chapter identifies the unintended side effects of targeting cryptomarkets. First, it analyses those unintended side effects. In addition, this chapter examines how significant those side effects are and how it impacts the society. Lastly, it explores how targeting cryptomarkets will force online vendors and consumers to adopt conventional drug distribution.

7.1 – Ramifications of Disrupting Cryptomarkets

According to Martin (2013), law enforcement agencies believe that it is vital to target and minimise the rapid growth of buyers and sellers in cryptomarkets. Hence, law enforcement officials have had numerous attempts to seize and shut

down online drug bazaars (Martin, 2014; Aldridge and Decary-Hetu, 2014; Barratt et al., 2014). For instance, as noted in Chapter 6, through an undercover operation, the FBI has seized and closed Silk Road 1.0. Despite the fact that the FBI successfully shut down the Silk Road 1.0 website, they were not able to reduce the number of consumers and distributors (Martin, 2014; Aldridge and Decary-Hetu, 2014). This indicates that law enforcement agencies have had very little impact in minimising the population of buyers and sellers online. According to Barratt et al. (2013), disrupting and targeting cryptomarkets tends to be problematic for law enforcement agencies, as there are numerous unintended side effects. For instance, the study of Aldridge and Decary (2014) has shown that targeting cryptomarkets would not reduce the number of sales and distributions; in fact, it would lead to more online drug sales.

It is therefore crucial to investigate and explore the unintended side effects of targeting cryptomarkets and how significant those side effects are for governments, law enforcement agencies and most profoundly for drug-users. Research has shown that while the aim of governments and law enforcement agencies is to permanently seize and shut down cryptomarkets (Barratt et al., 2013; Christin, 2012), there are also several negative consequences associated with such action (Martin, 2014; Aldridge and Decary-Hetu, 2014; Barratt et al., 2014; Martin, 2013; Van Hout and Bingham, 2013; Barratt et al., 2013). Barratt et al. (2013), for instance, argue that targeting cryptomarkets would create further issues for government, law enforcement agencies, public health and drug-users.

7.1.1 – Likely Impact of Targeting Cryptomarkets

Since the closure of the Silk Road 1.0 website, policing authorities have displaced more than 13,600 drug dealers (Benson, 2014). This suggests that the fall of the Silk Road website forced vendors and consumers to enter other cryptomarkets to obtain and distribute illicit goods. Despite the fact that the FBI closed Silk Road 1.0, there are more cryptomarkets and illicit drugs available than before the arrest of the alleged owner (Ross Ulbricht) of the website (Benson, 2014). This also suggests that while such action was carried out with positive intention, it had numerous negative or unintended side effects (Barratt et al., 2013).

First, law enforcement agencies have spent a substantial amount of money to investigate and seize Silk Road. In spite of spending this large sum of money, authorities have failed to prevent individuals from redeveloping the second version of the website (Silk Road 2.0). This suggests that targeting cryptomarkets is not an effective solution, as it would not prevent individuals from buying and selling illicit goods (Martin, 2014; Aldridge and Decary-Hetu, 2014; Benson, 2014; Van Hout and Bingham, 2013; Barratt et al., 2013; Martin, 2013). Targeting cryptomarkets forces distributors and consumers to relocate to other cryptomarkets. For example, recently, law enforcement officials have seized and closed the Utopia website (another online drug market). Soon after the closure of Utopia, Silk Road 2.0 saw an increase in the number of users (Global Drug Policy Observatory, 2014). This suggests that law enforcement officials have forced actors of Utopia to move to other cryptomarkets such as Silk Road 2.0 and Agora. Similarly, the recent seizure of Silk Road 1.0 has also

forced distributors and consumers to shift to other cryptomarkets. According to a recent report (Benson, 2014) published by the Digital Citizens Alliance, after the seizure of Silk Road 1.0, Agora is considered to be the successor of the Silk Road 1.0 website – implying that it is the current leader of the online drug market. Also the seizure of cryptomarkets would lead administrators and vendors to redevelop similar or more advanced websites.

Moreover, Martin (2013) argues that targeting cryptomarkets would force online vendors to adopt conventional forms of drug dealing and further exacerbate the situation for law enforcement agencies. As mentioned in Chapter 5, targeting these lucrative online drug bazaars may also increase systemic drug-related violence (Martin, 2014; Aldridge and Decary-Hetu, 2014; Martin, 2013; Van Hout and Bingham 2013). This suggests that rather than spending significant amounts of money and time to target these sites, governments and law enforcement agencies should shift their focus more towards targeting traditional drug dealing. It is deduced by Thoumi (2005) that the international drug market is estimated to be 500 billion US dollars. The figure provided by Thoumi (2005) suggests that cryptomarkets may be a less significant issue compared to the overall international drug market. This is because the worldwide distribution of illicit drugs facilitated through cryptomarkets is relatively low compared to the overall international drug market (Aldridge and Decary-Hetu, 2014; Martin, 2013). Countries, in particular third world countries that have limited communication infrastructure, may not be able to participate and access these lucrative online drug bazaars. For instance, Afghan farmers who cultivate raw opium may not be able to distribute their goods via cryptomarkets. In order to

distribute their goods, they tend to connect to broader distribution networks through intermediaries (Martin, 2013, p. 14). *"This indicates that online communications and cryptomarket technologies are not yet capable of eliminating completely the involvement of intermediary nodes across the world's various drugs markets"* (Martin, 2013, p. 14). Further research is necessary to determine whether cryptomarkets have an impact in reducing traditional drug distribution and other drug markets.

Currently, activities of cryptomarkets may have little or no impact in reducing conventional drug distribution; however, this will not necessarily remain the case for long, as empirical evidence (Martin, 2014; Decary-Hetu, 2014; Barratt et al., 2014; Van Hout and Bingham, 2013; Martin, 2013; Barratt et al., 2013 Christin, 2012) suggests that activities of cryptomarkets are rapidly increasing. In order to disrupt and target activities of cryptomarkets, it is significantly important for governments and law enforcement officials to strengthen their national borders and conduct thorough scans on each item that is travelling through traditional post. Through this process, law enforcement agencies and border protection agencies may have a fair chance to intercept more drugs and disrupt (to a certain degree) activities of cryptomarkets, as it tends to be more practical and effective. As noted in the preceding chapter, there are a number of issues associated with this strategy.

7.1.2 – Conclusion

Despite the fact that law enforcement agencies target this new breed of drug markets with positive intent, there are a number of unintended side effects

associated with such action. First, it does not minimise the rapid proliferation of buyers and sellers. This is due to the fact that buyers and sellers will shift to other cryptomarkets to conduct illicit transactions. Moreover, the seizure of a specific cryptomarket would force the administrators and vendors of sites to reestablish similar or more advanced websites. Not only that, targeting cryptomarkets would force buyers and sellers to exchange illicit goods in a conventional manner (i.e., wholesaler, distributor, street dealer). This would not only increase systemic drug-related violence, it may also increase drug-related harm and mortality rates.

Chapter 8: Conclusions and Future Directions

The preceding chapters have analysed and explored cryptomarkets from a variety of conceptual and empirical perspectives. Considering all the empirical evidence, it seems as though cryptomarkets are in the process of redefining and changing the nature of the illicit drug trade (Martin, 2014; Barratt et al., 2014; Aldridge and Decary-Hetu, 2014; Van Hout and Bingham, 2013; Martin, 2013; Van Hout and Bingham, 2013a; Barratt et al., 2013; Van Hout and Bingham, 2013b; Christin, 2012; Barratt, 2012). This is due to the fact that modern and sophisticated computer technologies allow administrators, vendors and consumers to anonymously obtain and distribute illicit goods via the Internet and to a great extent out of reach of law enforcement. Therefore, the development of cryptomarkets is a significant issue, as it is a novel way of distributing and acquiring illicit goods via the Internet. This chapter offers concluding comments on why it is advisable for law enforcement agencies not to target cryptomarkets. First, it discusses that the perceptions of the media, law enforcement agencies and academics in regards to cryptomarkets and how they create misconceptions in society. Moreover, this chapter discusses the significance of cryptomarkets in contemporary society and why law enforcement officials should not target them. Finally, the chapter offers concluding comments on the unintended side effects of targeting these online illicit drug bazaars.

8.1 – Research Findings

This research has examined and explored various facets of cryptomarkets. By analysing all the empirical evidence in the preceding chapters, this thesis

concludes that the media tends to use persuasive language to create moral panic amongst the general public, manipulate public perceptions, dominate market share and maintain their audience. In the case of cryptomarkets, the media continuously depict the development of these online illicit markets out of proportion by using emotive language (e.g., eBay for drugs) to create fear in society and portray a negative image of law enforcement agencies. Since the development of cryptomarkets, commentators constantly portray this new breed of drug market as a significant issue, although this research demonstrated that cryptomarkets are a less significant issue when compared to the traditional illicit drug trade.

Furthermore, law enforcement agencies believe that these illicit drug markets are not a new phenomenon and therefore perceive cryptomarkets as a drug-related issue, rather than perceiving the initial stages of this lucrative drug market as a cyber-related issue. This is a significant issue, because in order to understand the illicit nature and the encrypted stages of cryptomarkets, law enforcement agencies should change their perception towards this innovative form of illicit drug trade. It may be more useful, therefore, if law enforcement agencies should start conceptualising the activities of cryptomarkets from the perspective of cybercrime.

On other hand, scholars perceive that cryptomarkets are a less violent alternative to conventional drug distribution networks. As findings of this research demonstrated in preceding chapters, scholars (Martin, 2014; Aldridge and Decary-Hetu, 2014; Van Hout and Bingham, 2013; Martin, 2013; Van Hout and

Bingham, 2013b; Barratt et al., 2013; Christin, 2012) maintain a positive description of cryptomarkets. Since the development of cryptomarkets, scholars stated that they are an innovative platform that allows drug distributors and drug-users to maintain anonymity while conducting illicit transactions via the Internet. This suggests that cryptomarkets offer various advantages for vendors and drug-users to safely and cheaply distribute or obtain illicit goods when compared to the conventional forms of drug trade. Due to these advantages and safety measures, cryptomarkets differ significantly from conventional forms of drug distribution.

Taking that into account, this research argues that law enforcement agencies should not disrupt or target cryptomarkets and instead should shift their focus towards disrupting or targeting the traditional illicit drug market. This is due to the fact that disrupting or targeting cryptomarkets would force administrators, producers, vendors and consumers to redevelop alternative sites or relocate to other cryptomarkets. Even if law enforcement authorities disrupt the entire infrastructure of cryptomarkets, then traditional drug distribution would likely take its place. This would further complicate the situation for policing authorities to combat illicit drugs, because traditional drug distribution would increase the risk of more organised criminal activities in communities.

In addition, by analysing Australian drug policies, this research further concludes that cryptomarkets should not be targeted under the current drug policy of Australia. First, the analysis of this research revealed that there is no specific reference to cryptomarkets in the existing drug policy of Australia. The

significance of analysing cryptomarkets through current Australian drug policy further revealed that the cryptomarkets reflect and reinforce certain aspects of the current drug policy of Australia. Disrupting cryptomarkets under current Australian drug policy would have negative implications for the Australian Government, the Australian Institute of Health and Welfare, Australian communities and more importantly drug-users. Empirical evidence (Barratt et al., 2013) suggests that disrupting cryptomarkets would shift drug-related discussion to social media (e.g., Facebook and Twitter) and other proprietary operating systems on mobile devices.

Law enforcement agencies may not agree with the findings of this research. This is due to the fact that it is their responsibility to maintain law and order and prevent individuals from committing illicit activities. Due to the illicit nature of cryptomarkets, law enforcement authorities are dedicated to disrupt and/or target these illicit drug bazaars. However, empirical evidence suggests that it is immensely difficult for policing authorities to disrupt and/or target cryptomarkets (Martin, 2014; Aldridge and Decary-Hetu, 2014; Van Hout and Bingham, 2013; Martin, 2013; Van Hout and Bingham, 2013b; Barratt et al., 2013; Christin, 2012). First, the rapid emergence of advanced and more secure cryptomarkets suggests that law enforcement agencies are largely failing to reduce the overall number of these illicit drug bazaars. The reason behind this failure is that the current intervention strategies have proven to be ineffective, expensive, time consuming and significantly difficult to implement. To date, the only intervention strategy that had a short-term impact in disrupting the operations of cryptomarkets is undercover investigation. The reason that

undercover investigation had a short-term impact is that the closure of Silk Road 1.0 and Utopia did not prevent administrators and vendors of these sites developing Silk Road 2.0. (Martin, 2014; Aldridge and Decary-Hetu, 2014; Benson, 2014; Van Hout and Bingham, 2013; Barratt et al., 2013; Martin, 2013).

The emergence of new cryptomarkets (e.g., Silk Road 2.0) suggests that there are a number of unintended side effects associated with targeting these online drug bazaars. First, targeting cryptomarkets would likely increase drug-related harm, mortality rates, drug-related diseases and systemic drug-related violence. Organised crime may also increase in communities. This is due to the fact that organised crime groups get involved in violent activities to dominate market share, resolve conflicts and protect territories. In addition, as this research demonstrated in preceding chapters, disrupting cryptomarkets would impede drug-users from living normal and useful lives as full members of the community. Drug-users would not have detailed drug-related information and they may not participate in government-funded harm reduction programs. These unintended side effects are significant, as they tend to destabilise communities, including those in Australia.

8.1.1 – Limitations of the Project

This research project has certain limitations. One of the limitations associated with this study is the fact that it relied and focused on secondary data. This is due to the fact that obtaining ethical approval for this research may have taken a significant amount of time. In order to overcome this obstacle, the researcher relied and focused on data collected by other authors. Another limitation of this

research project is that due to time constraints and a restricted word count, this study analysed cryptomarkets only through current Australian drug policy. Furthermore, online illicit drug trade is a new area and important issue in contemporary society. It requires further investigation to find new facts and figures about different facets of this new breed of drug trade.

8.1.2 – Future Work

As previously mentioned, the development of cryptomarkets is a new criminological phenomenon that requires further research. For future direction, it may be useful to analyse cryptomarkets through other Western (e.g., United Kingdom, France, Germany, Netherlands, America, Canada etc.) drug policies to determine whether these online drug markets reinforce and reflect certain aspects of those drug policies or not. It is also critically important to estimate the value of cryptomarkets in the international illicit drug market. The significance of estimating the value of cryptomarkets will determine whether cryptomarkets have an impact in reducing traditional drug distribution and other drug markets. In addition, at this stage, it seems that the development of cryptomarkets may possibly transform the international illicit drug trade. This may affect producers, distributors, consumers, as well as governments, law enforcement agencies and the general public. Thus, it requires further research to determine if the online illicit drug trade would entirely change the means of illicit drug distribution.

References

Aldridge, J. & Decary-Hetu, D. (2014) *Not an Ebay for Drugs: The Cryptomarket 'Silk Road' as a Paradigm Shifting Criminal Innovation.* (Online) Available at: http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2436643

(Accessed on: 26/06/2014)

Agren, D. (2010) *Mexico: Death Toll from Drug-related Violence is Thousands Higher than was Reported Earlier. New York Times.* (Online) Available at: http://www.nytimes.com/2010/08/04/world/americas/04forbriefs-MEXICO.html

(Accessed on 10/07/2014)

Australian Bureau of Statistics (2005) *Drug Related Deaths: Drug related Deaths by Type of Drugs. Drug Free Australia.* (Online) Available at: http://www.drugfree.org.au/fileadmin/Media/Reference/DFA_DrugRelatedStats.pdf

(Accessed on: 14/08/2014)

Australian Institute of Health and Welfare. (2011). *2010 National Drug Strategy Household Survey* (Drug statistics series no. 25. Cat. no. PHE 145). Canberra, Australia: Author.

Australian Medical Association. (2013) *The Rise of Drug Overdose. Australian Medicine.* (Online) Available at: https://ama.com.au/ausmed/rise-drug-overdoses

(Accessed on: 22/07/2014)

Australia Post. (2013) *Australia Post Annual Report. Future Ready.* (Online) Available at: http://auspost.com.au/annualreport2013/downloads.html (Accessed on: 02/07/2014)

Bailey, M., Cook, E., Jahanian, F., Myrick, A. & Sinha, S. (2006) *Practical Darknet Measurement. Information Sciences and Systems, 40th Annual Conference,* pp. 1496-1501.

Balkin, J. M., Grimmelmann, J., Katz, E., Kozlovski, N., Wagman, S. & Zarsky, T. (2006) *Cybercrime. Digital Cops in a Network Environment. New York University Press,* New York, United States of America.

Barak, A. & King, S. A. (2000) *The Two Faces of the Internet: Introduction to the Special Issue on the Internet and Sexuality. CyberPsychology and Behaviour,* Vol. 3, No. 4, pp. 517-520.

Barnet, E. R. (2014) *Virtual Currencies: Safe for Business and Consumers or Just for Criminals. 13th European Security Conference & Exhibition.* (Online) Available at: http://photos.state.gov/libraries/useu/231771/PDFs/2014_Erik_Barnett_crypto-currencies_remarks.pdf (Accessed on: 01/05/2014)

Barratt, M. J. (2012a). *The Efficacy of Interviewing Young Drug Users through Online Chat. Drug and Alcohol Review,* Vol. 31, pp. 566-572.

Barratt, M. (2012) *Letters to the Editor: 'Silk Road: eBay for Drugs'. Addiction 107,* pp. 683-684.

Barratt, M., Lenton, S. & Allen, M. (2013) *Internet Content Regulation, Public Drug Websites and the Growth in Hidden Internet Services. Drugs. Education, Prevention and Policy,* Vol. 20, No. 3, pp. 195-20.

Barratt, M., Ferris, J. & Winstock, A. (2014) *Use of Silk Road, the Online Drug Marketplace, in the United Kingdom, Australia and the United States. Addiction 109,* pp. 774-783.

Basu, G. (2014) *The Strategic Attributes of Transnational Smuggling: Logistics Flexibility and Operational Stealth in the Facilitation of Illicit Trade. Journal of Transportation,* Vol. 7, No. 2, pp 99-113.

BBC News. (2014) *Who is Behind Mexico's Drug Related Violence?* (Online) Available at: http://www.bbc.com/news/world-latin-america-10681249 (Accessed on: 07/08/2014)

Benson, A. (2014) *More Illegal Drugs Now Available on the "Silk Road" than Before Arrests: Six Months After the FBI Captured the Alleged "Dread Pirate*

Roberts", the Digital Citizens Alliance Report Investigates the State of the "Silk Road" and Other Darknet Markets. Digital Citizens Alliance.

Berthier, R. & Cukier, M. (2008) *The Development of a Darknet on an Organization-Wide Network: An Empirical Analysis. High Assurance Systems Engineering and Symposium Conference,* pp. 59-68.

Bethencourt, J., Low, W. Y., Simmons, I. & Williamson, M. (2007) *Establishing Darknet Connections: An Evaluation of Usability and Security. Proceedings of the 3rd ACM International Symposium on Usable Privacy and Security,* Vol. 229, pp. 145-146.

Birdsey, E. M. (2012) *Criminal Offences Involving Firearms in New South Wales, 1995–2011.* NSW Bureau of Crime Statistics and Research. *Crime and Justice Statistics.*

Blumstein, A. (1995) *Youth Violence, Guns, and the Illicit-Drug Industry. Journal of Criminal Law and Criminology,* Vol. 86, No. 1, pp. 10-36.

Bouchard, M. & Tremblay, P. (2005) *Risks of Arrest Across Drug Markets: A Capture-Recapture Analysis of "Hidden" Dealer and User Populations. Journal of Drug Issues,* Vol. 35, No. 4, pp. 733-754.

Bouchard, M. (2007) *A Capture-Recapture Model to Estimate the Size of Criminal Populations and the Risks of Detection in a Marijuana Cultivation Industry. Journal of Quantitative Criminology,* Vol. 23, No. 3, pp. 221-241.

Bryman, A. (2008) *Social Research Methods,* 3rd ed. *Oxford University Press,* New York, United States of America.

Bush, W., Roberts, M. & Trace, M. (2004) *Upheavals in the Australian drug market: heroin drought, stimulant flood. The Beckley Foundation Drug Policy Programmee, Drugscope briefing paper* No. 4.

Castle, A. (2009) *Statistical Overview of Homicides in British Columbia, 1997–2007: 2009 Update.* Vancouver: Royal Canadian Mounted Police.

Caulkins, J. & Reuter, P. (2009) *Towards a Harm-Reduction Approach to Enforcement. Safer Communities,* Vol. 8, No. 1, pp. 9-23.

Christin, N. (2012) *Travelling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace. Working Paper,* Carnegie Mellon.

Decker, S. H. (2003) *Policing Gangs and Youth Violence. Wadsworth Publishing Co,* United States of America.

Denscombe, M. (2009) *Ground Rules for Social Research: Guidelines for Good Practice,* 2nd ed. *McGraw-Hill Custom Publishing,* Sydney, Australia.

Dowler, K. (2003) *Media Consumption and Public Attitudes Toward Crime and Justice: The Relationship Between Fear of Crime, Punitive Attitudes, and Perceived Police Effectiveness. Journal of criminal justice and popular culture,* Vol. 10, No. 2, pp. 109-126.

Duff, C. (2004) *Drug use as a 'practice of self': is there any place for an 'ethics of moderation' in contemporary drug policy?. International Journal of Drug Policy,* Vol. 15, pp. 385-393.

Furnell, S. (2002) *Cybercrime: Vandalizing the Information Society. Addison Wesley,* London, England.

Global Drug Policy Observatory. (2014) *Law Enforcement is Currently not the Greatest Threat to the Survival of Darknet Drug Markets. Reporting and monitoring analysis.* (Online) Available at: http://www.swansea.ac.uk/media/GDPO%20SA%20Darknet%20Threats%20FINAL.pdf
(Accessed on: 21/09/2014)

Goldstein, J. (2013) *Arrest in U.S. Shuts down a Black Market for Narcotics.* New *York Times.* (Online) Available at: http://www.nytimes.com/2013/10/03/nyregion/operator-of-online-market-for-illegal-drugs-is-charged-fbi-says.html?_r=2&
(Accessed on: 14/08/2014)

Goldstein, M. (2014) *Silk Road Case Began With Hunt for a John Deo. The New York Times* (Online) Available at: http://dealbook.nytimes.com/2014/03/21/silk-road-case-began-with-hunt-for-a-john-doe/?_php=true&_type=blogs&_r=0 (Accessed on 28/08/2014)

Grabosky, P. (2001) *Virtual Criminality: Old Wine in New Bottles? Social & legal Studies,* Vol. 10, pp. 243-9.

Grabosky, P. (2007) *Requirements of Prosecution Services to Deal with Cyber Crime*. *Crime Law Soc Change,* Vol. 47, pp. 201-203.

Harper, D, W. & Frailing, K. (2010) *Crime and Criminal Justice in Disaster*. *Carolina Academic Press,* North Carolina, United States of America.

Hewson, C. (2006) *Secondary Analysis,* in Jupp, V. (ed.), *The Sage Dictionary of Research Methods*. *Sage,* London.

Hutson, H. R., Anglin, D., Kyriacou, D., Hart, J. & Spears, K. (1995) *The Epidemic of Gang-related Homicides in Los Angeles County from 1979 through 1994*. *JAMA,* 274(13), 6.

Jaishankar, K. (2011) *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior. CRC Press,* Florida, United States of America.

Jenner, M. S. (2011) *International Drug Trafficking: A global problem with a domestic solution. Indiana Journal of Global legal Studies,* Vol. 18, No. 2, pp. 901-927.

Jewkes, Y. & Yar, M. (2010) *The Internet, Cybercrime and the Challenges of the Twenty-first Century.* In: Jewkes, Y. & Yar, M. (eds) *Handbook of Internet Crime.* Devon: *Willan Publishing.*

Johnson, B. D., Golub, A. & Dunlap, E. (2000) *The Rise and Decline of Hard Drugs, Drug Markets and Violence in Inner-city New York.* In Blumstein, A. & Wallman, J. (eds.), *The crime drop in America* (pp. 164-206). *Cambridge University Press,* Cambridge, United Kingdom.

Kien-Meng Ly, M. (2014) *Coining Bitcoin's "Legal-Bits": Examining the Regulatory Framework for Bitcoin and Virtual Currencies. Harvard Journal of Law & Technology,* Vol. 27, No. 2, pp. 588-608.

King, J. (2004) *Deep Web Collection Section.* (Online) Available at: http://eprints.qut.edu.au/15992/3/John_King_Thesis.pdf
(Accessed on: 23/08/2014)

Leaning, M. (2009) *The Internet, Power and Society: Rethinking the power of the Internet to change lives*. *Woodhead Publishing Ltd,* Oxford, England.

Levitt, S. D. & Venkatesh, S. A. (2000) *An Economic Analysis of a Drug-Selling Gang's Finances. The Quarterly Journal of Economics,* Vol. 115, No. 3, pp. 755-789.

Mansfield, R. (2013) *Silk Road: Accessing the 'Drugs eBay' Was Easy. Sky News.* (Online) Available at: http://news.sky.com/story/1149755/silk-road-accessing-the-drugs-ebay-was-easy
(Accessed on: 14/08/2014)

Martin, J. (2013) *Lost on the Silk Road: Online Drug Distribution and the 'Cryptomarket'. Criminology and Criminal Justice:* 1748895813505234.

Martin, J. (2014) *Drugs on the Dark Net: How Cryptomarkets Are Transforming the Global Trade in Illicit Drugs. Palgrave Macmillan,* United Kingdom.

Martin, I., Palepu, A., Wood, E., Li, K., Montaner, J. & Kerr, T. (2009) *Violence Among Street-Involved Youth: The Role of Methamphetamine. European Addiction Research,* Vol.15, No.1, pp. 32-38.

McCusker, R. (2007) *Transnational Organised cyber crime: Distinguishing Threats from Reality. Crime Law Soc Change,* Vol. 46, pp. 257-273.

Mclntyre, L. (2014) *Cyber-Takings: The War on Crime Moves into the Cloud. Journal of Technology Law and Policy,* Vol. 14, pp. 333-350.

McNeilage, A., Levy, M. & Hall, L. (2014) *Police Claim to Know about all Sydney Shootings After Brothers 4 Life Arrests. The Sydney Morning Herald.* (Online) Available at: http://www.smh.com.au/nsw/police-claim-to-know-about-all-sydney-shootings-after-brothers-4-life-arrests-20140109-30is4.html
(Accessed on: 15/08/2014)

Moore, T. J. (2008) *The Size and Mix of Government Spending on Illicit Drug Policy in Australia. Drug and Alcohol Review,* Vol. 27, pp. 404-413.

Moses, A. (2012) *'Dark Net' Drug Deals Boom on Cyber Silk Road. The Sydney Morning Herald.* (Online) Available at: http://www.smh.com.au/technology/technology-news/dark-net-drug-deals-boom-on-cyber-silk-road-20120810-23wdj.html
(Accessed on 10/10/2014)

Murdoch, S. (2006) *Hot or Not: Revealing Hidden Services by their Clock Skew. In Proceedings of the 13th ACM conference on Computer and Communications Security.* Alexandria, VA, pp. 27-36.

Nakamoto, S. (2008) *Bitcoin: A Peer-to-Peer Electronic Cash System.* (Online) Available at: https://bitcoin.org/bitcoin.pdf
(Accessed on: 07/06/2014)

National Drug and Alcohol Research Centre. (2013) *Law Enforcement Takes the Lion's Share of Illicit Drug Spend. Media Release.* (Online) Available at:

http://ndarc.med.unsw.edu.au/news/law-enforcement-takes-lion's-share-illicit-drug-spend

(Accessed on: 18/07/2014)

National Drug and Alcohol Research Centre. (2014) *Australian Use of Underground Illicit Drug Websites Jumps. Media Release.* (Online) Available at: https://ndarc.med.unsw.edu.au/news/australian-use-underground-illicit-drug-websites-jumps

(Accessed on: 16/06/2014)

Nossal, G., Hamilton, M., Kirby, M. & Penington, D. (2012) *Australian Drug Policy: Harm reduction and new recovery.* (Online) Available at: http://www.anex.org.au/wp-content/uploads/2011/09/Australian-Drug-Policy-harm-reduction-and-new-recovery-April-2012.pdf

(Accessed on: 01/04/2014)

O'Leary, Z. (2004) *The Essential Guide to Doing Research. Sage Publications,* London, United Kingdom.

Ormsby, E. (2012) *The Drug's in the Mail. The Age.* (Online) Available at: http://www.theage.com.au/victoria/the-drugs-in-the-mail-20120426-1xnth.html

(Accessed on: 02/09/2014)

Ousey, G. C. & Lee, M. R. (2004) *Investigating the Connections Between Race, Illicit Drug Markets, and Lethal Violence, 1984-1997. Journal of Research in Crime and Delinquency,* Vol. 41, No. 4.

Overlier, L. & Syverson, P. (2006) *Locating Hidden Servers. In Proceedings of the 2006 IEEE Symposium on Security and Privacy.* Oakland, CA, pp. 100-144.

Paul Gee, J. (2011) *An Introduction to Discourse Analysis: Theory and Method. Routledge,* New York, United States of America.

Paul Gee, J. (2014) *Discourse Analysis: Theory and Method. Routledge,* New York, United States of America.

Pauli, D. (2012) *Aussie Coppers Bedeviled by Online Contraband Networks. SC Magazine.* (Online) Available at: http://www.itnews.com.au/News/314984,aussie-coppers-bedeviled-by-online-contraband-networks.aspx
(Accessed on: 10/10/2014)

Perry, D. E., Porter, A. A. & Votta, L, G. (2000) *Empirical Studies of Software Engineering: A Roadmap. Proceedings of the Conference on the Future of Software engineering.* Limerick, Ireland, pp. 345-355.

Phelps, A. & Watt, A. (2014) *I Shop Online – Recreationally: Internet Anonymity and Silk Road Enabling Drug Use in Australia. Digital Investigation,* pp. 1-12.

Power, M. (2013) *Life After Silk Road: How the Darknet Drug Market is Booming. The guardian.* (Online) Available at: http://www.theguardian.com/technology/2014/may/30/life-after-silk-road-how-the-darknet-drugs-market-is-booming
(Accessed on: 10/10/2014)

Quarantiello, L. E. (1997) *How to Protect Yourself from Computer Criminals. LimeLight Books,* New York, United States of America.

Ren, L. (2014) *Proof of Stake Velocity: Building the Social Currency of the Digital Age.* (Online) Available at: https://www.reddcoin.com/papers/PoSV.pdf
(Accessed on: 28/08/2014)

Reuter, P. (2009) *Systemic Violence in Drug Markets. Crime Law Soc Change,* Vol. 52, No. 3, pp. 1-10.

Reuter, P. & Kleiman, M. (1986) *Risks and Prices: An Economic Analysis of Drug Environment. Crime and Justice,* Vol. 7, pp. 289-340.

Roberts, J. & Doob, A. (1986) *Public Estimates of Recidivism Rates: Consequences of a Criminal Stereotype. Canadian Journal of Criminology,* Vol. 28, pp. 229-241.

Robinson, M. (2012) *The eBay for Drugs: 'Silk Road' Website Allows UK Drug Users to Buy Cocaine and Heroin by Mail Order from all Over the World. Daily Mail Australia.* (Online) Available at: http://www.dailymail.co.uk/news/article-2235199/The-eBay-drugs-Silk-Road-website-allows-drug-users-buy-heroin-cannabis-mail-order-world.html
(Accessed on: 14/08/2014)

Romero-Daza, N., Weeks, M. & Singer, M. (2003) *"Nobody Gives a Damn if I Live or Die": Violence, Drugs, and Street-level Prostitution in Inner-city Hartford, Connecticut. Medical Anthropology,* Vol. 22, No. 3.

Schiffrin, D. Tannen, D. & Hamilton, H. E. (2001) *The Handbook of Discourse Analysis. Blackwell Publishers Ltd,* Massachusetts, United States of America.

Seaman, C. (1999) *Qualitative Methods in Empirical Studies of Software Engineering. IEEE Transactions on Software Engineering,* Vol. 25, No. 4, pp. 557-572.

Smith, H. (2014) *Bitcoin Traders Charged Over Silk Road, 'The eBay of Drugs'. Metro News.* (Online) Available at: http://metro.co.uk/2014/01/27/bitcoin-traders-charged-over-silk-road-the-ebay-of-drugs-4279776/

(Accessed on: 14/08/2014)

Spear, N. (2014) *Crypto-currencies: A Most Unusual Rhetoric.* (Online) Available at: http://courses.rhetorike.org/sherrill2/system/files/Nathan%20Spear%20Revised.pdf

(Accessed on 12/04/2014)

Surette, R. (1998) *Media, Crime, and Criminal Justice: Images and Realities* 2nd ed. *Wadsworth Publishing,* New York, United States of America.

Sutton, C. (2013) *Bikie Nation: The Outlaw Gangs in Your Backyard.* Nation News. (Online) Available at: http://www.news.com.au/national/bikie-nation-8212-the-outlaw-gangs-in-your-backyard/story-fncynjr2-1226690598400

(Accessed on: 07/08/2014)

Swearingen, J. (2014) *A Year After the Death of Silk Road, Darknet Markets are Booming. The Atlantic.* (Online) Available at: http://www.theatlantic.com/technology/archive/2014/10/a-year-after-death-of-silk-road-darknet-markets-are-booming/380996/

(Accessed on: 10/10/2014)

The Australian Federal Police. (2012) Media Release: AFP and Customs Warn Users of Silk Road. (Online) Available at: http://www.afp.gov.au/media-centre/news/afp/2012/july/afp-and-customs-warn-users-of-silk-road.aspx

(Accessed on: 03/08/2014)

Thomas, D. and Loader, B. (2000) *Introduction – Cybercrime: Law Enforcement,*

Security and Surveillance in the Information Age. In D. Thomas and B. Loader (eds) *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age. Routledge,* London, England.

Thoumi, F. E. (2005) *The Colombian Competitive Advantage in Illegal Drugs: The role of policies and institutional changes. Journal of Drug Issues,* Vol. 35, No. 1, pp. 7-26.

Trimingham, T. (2012) *Alternatives to Prohibition. Illicit Drugs: How We Can Stop Killing and Criminalising Young Australians.* (Online) Available at: http://www.australia21.org.au/publication-archive/alternatives-to-prohibition-illicit-drugs-how-we-can-stop-killing-and-criminalising-young-australians-australia21-canberra/#.UmXFZuBK670

(Accessed on 01/06/2014)

United Nations Office on Drugs and Crime. (2014) *World Drug Report.* (Online) Available at: https://www.unodc.org/documents/wdr2014/World_Drug_Report_2014_web.pdf

(Accessed on: 28/08/2014)

Van Buskirk, J. Roxburgh, A. Bruno, R. & Burns, L. (2013) *Drugs and the Internet.* The national illicit drug indicators project, National Drug and Alcohol Research Centre. (Online) Available at: https://ndarc.med.unsw.edu.au/sites/default/files/ndarc/resources/DrugsTheInternet_Newsletter%20FINAL%20with%20ISSN.pdf
(Accessed on: 03/07/2014)

Van Buskrik, J., Roxburgh, A., Farrell, M. & Burns, L. (2014) *The Closure of Silk Road: What has this Meant for Online Drug Trading? Addiction,* Vol. 109, No. 4, pp. 517-518.

Van Hout, M. & Bingham, T. (2013) *Silk Road, the Virtual Drug Marketplace: A Single Case Study of User Experiences. International Journal of Drug Policy.* (Online) Available at: http://dx.doi.org/10.1016/j.drugpo.2013.01.005.
(Accessed on: 29/02/2014)

Van Hout, M. & Bingham, T. (2013a) *Surfing the Silk Road: A Study of Users Experiences. International Journal of Drug Policy,* Vol. 24, pp. 524-529.

Van Hout, M. & Bingham, T. (2013b) *Responsible Vendors, Intelligent Consumers: Silk Road, the Online Revolution in Drug Trading.* International Journal of Drug Policy. (Online) Available at: http://dx.doi.org/10.1016/j.drugpo.2013.10.009
(Accessed on 16/04/2014)

Wakefield, J. (2014) *Huge Raid to Shut Down 400-plus Dark Net Sites. BBC News.* (Online) Available at: http://www.bbc.com/news/technology-29950946 Accessed on (21/11/2014)

Wall, D. (2001) *Cybercrimes and the Internet.* In D. Wall (ed.) *Crime and the Internet. Routledge,* London, England.

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

Wall, D. (2010) *The Internet as a Conduit for Criminal Activity.* (Online) Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=740626 (Accessed on 07/06/2014)

Werb, D., Rowell, G., Guyatt, G., Kerr, T., Montaner, J. & Wood, E. (2011) *Effect of Drug Law Enforcement on Drug Market Violence: A systematic Review. International Journal of Drug Policy,* Vol. 22, No. 2, pp. 87-94.

Wright, A. (2008) *Searching the Deep Web: While the Semantic Web may be a Long Time Coming, Deep Web Search Strategies Offer the Promise of a Semantic Web. Technology,* Vol. 51, No 10, pp. 14-15.

Yar, M. (2005) *The Novelty of Cybercrime: An Assessment in Light of Routine Activity Theory. European Journal of Criminology,* Vol. 2, No. 4, pp. 407-427.

Zheng, R., Qin, Y., Huang, Z. & Chen, H. (2003) *Authorship Analysis in Cybercrime Investigation. Springer-Verlag Berlin,* Vol. 2665, pp. 59-73.