Vincent Harinam
Barak Ariel

Law Enforcement Strategies for Disrupting Cryptomarkets

A Practical Guide to Network Structure, Trust Dynamics, and Agent-Based Modelling Approaches

Springer

Law Enforcement Strategies for Disrupting Cryptomarkets

Vincent Harinam • Barak Ariel

Law Enforcement Strategies for Disrupting Cryptomarkets

A Practical Guide to Network Structure, Trust Dynamics, and Agent-Based Modelling Approaches

Springer

Vincent Harinam
Independent Researcher
Mournival Applied Research
Calgary, AB, Canada

Barak Ariel
The Hebrew University of Jerusalem
Jerusalem, Israel

University of Cambridge
Cambridge, UK

ISBN 978-3-031-62820-7 ISBN 978-3-031-62821-4 (eBook)
https://doi.org/10.1007/978-3-031-62821-4

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Contents

List of Figures

List of Tables

Chapter 1
Introduction

Introduction

Gone are the days when prospective consumers relied solely on local dealers to procure drugs and other illicit goods and services. The advent of digital encryption and Internet connectivity has facilitated the rise of cryptomarkets. Similar in function to Amazon or eBay, cryptomarkets are illicit online marketplaces hosted on the dark web that facilitate the exchange of illegal goods and services. Much like licit online markets, cryptomarkets allow those who wish to purchase illicit goods and services to do so from the comfort of their own homes, placing their order with a vendor and receiving the product through the postal service. Whether it be marijuana, cocaine, bladed implements or hitmen, these platforms are replete with a variety of illicit wares. Cryptomarkets represent a unique context: They facilitate traditional criminal dynamics and introduce new challenges for law enforcement. Moreover, these platforms present a novel opportunity for researchers to test the accuracy of key theoretical precepts applied to terrestrial markets.

Law enforcement agencies have often lagged behind criminal entities, especially in key areas such as cyber and finance (Curtis & Oxburgh, 2022). There are clear challenges posed by the emergence of cybercrimes, but police (and law enforcement) responses to these challenges have so far been limited. The police, as a social institution, are ill-equipped to manage cryptomarkets. In general, national or elite departments handle these illicit markets—which implies that only specialised law enforcement agents are capable and have the capacity to put a dent in this growing area of criminal business. The challenges to law enforcement are all too clear: International criminals that act outside jurisdictional boundaries, state actors with unlimited resources, technology-savvy organised crime groups, small and underfunded anti-cybercrime units and a lack of fundamental training in digital forensics are just some of the barriers to the effective police response to cybercrime in general and cryptomarkets more specifically (Giommoni et al., 2024). The Silk Road and

V. Harinam, B. Ariel, *Law Enforcement Strategies for Disrupting Cryptomarkets*,
https://doi.org/10.1007/978-3-031-62821-4_1

other darknet platforms earned billions before law enforcement brought them down (Dolliver, 2015). The regulation of initial cryptocurrency coin offerings—an area where fraud is prevalent (Tiwari et al., 2020)—and the regulation of binary options trading in which many innocent investors lost their money due to scams (Lacey et al., 2020) both emerged many years after scammers made billions of dollars off innocent investors. More recently, it was revealed that North Korean hackers allegedly stole hundreds of millions in crypto to fund nuclear programmes (Chiang, 2023), many years after the fact.

This book endeavours to push the cryptomarket literature beyond its present methodological limits by documenting the network structure of a cryptomarket and measuring the efficacy of targeted strategies on the transactional network of a cryptomarket. To this end, a combination of social network analysis and agent-based modelling is employed to build the transactional network structure of a cryptomarket and simulate its disruption through sequential node deletion. The overarching aim of this book is threefold. First, all cryptomarket interventions by law enforcement to date are documented and evaluated, providing a breakdown of their evolution and overall efficacy. Second, social network analysis and agent-based modelling will be presented as useful tools for police practitioners and crime researchers when measuring the impact of disruptive interventions to counter criminal networks. Third, the findings herein are used to inform targeted interventions by law enforcement against cryptomarkets. Past law enforcement strategies targeting cryptomarkets have been ineffective and, in some cases, counterproductive (Soska & Christin, 2015; Decary-Hetu & Giommoni, 2017; Van Buskirk et al., 2017). As such, this book explicitly focuses on adaptive simulations and the efficacy of law enforcement interventions. It aims to offer some insight into how law enforcement might structure their cryptomarket intervention strategies to achieve maximum long-term disruptive impact.

Book Structure and Chapter Overview

This book is divided into six chapters, with Chaps. 1 and 6 serving as the introductory and concluding chapters. Chapter 2 is an up-to-date summary of the extant cryptomarket literature, drawing upon a vast swathe of studies across a decade of research. No research questions are posed or analyses conducted in this chapter. The objective of this chapter is to define cryptomarkets and situate these illicit platforms within the cybercrime and organised crime contexts. A secondary objective is to take stock of the present state of cryptomarket research, tracking major scholarly themes across a decade of research. In short, an extensive overview of key themes within the cryptomarket literature is conducted. This provides a strong foundation for those new to the subject of cryptomarkets while also providing new insights to those who are well acquainted with the topic. Furthermore, one overarching benefit of conducting a state-of-the-art literature review is that substantive gaps in the literature can be identified.

Chapter 3 explores the various actions taken by law enforcement organisations against cryptomarkets as well as their measurable impact on the dark web ecosystem thereafter. This chapter delves into how law enforcement understands and engages in interventions against cryptomarkets, how actors on the dark web adjust their operations against disruptions and the implications of this dynamic on the overall dark web ecosystem in the interim and in the long term. Law enforcement's fragmentation of the dark web ecosystem and the inadvertent improvements to criminal efficiency post-intervention are discussed herein.

Chapter 4 seeks to disentangle trust dynamics in a dark web market, uncovering the processes by which trust is created and maintained and how this ultimately affects the network structure of the market. To this end, a battery of statistical analyses is applied to a cryptomarket transactional network to understand how trust is formed among buyers and vendors and how vendors create a lasting reputation on the platform. In addition, the aim is to understand the determinants of a buyer's decision to purchase on a cryptomarket and why specific vendors are chosen over others. Understanding the structural dynamics and transactional mechanisms between vendors and buyers is a pivotal first step in disrupting the ease of operation of a cryptomarket.

Finally, Chap. 5 examines the theoretical and practical elements of agent-based modelling (ABM) as a methodological and strategic tool to inform interventions against criminal organisations and networks. This chapter begins by explaining the intricacies and aims of agent-based modelling and then examines practical ABM use cases in various domains, with a special focus on law enforcement and criminal justice. This chapter also delves into the intricacies of designing an agent-based model. More specifically, a model which tests the effectiveness of several law enforcement strategies against a criminal network is designed, covering each of the necessary steps in this process. Finally, the results of the constructed agent-based model are examined, with the implications for law enforcement interventions being explained.

Data and Methodological Overview

This analysis in this book relies on a buyer-seller dataset from the Abraxas cryptomarket (Branwen et al., 2015). Apart from the anonymous cryptomarket analysed by Duxbury and Haynie (2017), this is the only marketplace where unique identifiers are available for buyers. As such, it was the only known publicly available dataset which allowed for network analysis and adaptive computer simulation. With assistance from Lukas Norbutas of Utrecht University and Cambridge University's Computer Laboratory, this data was extracted from a public data repository established by independent researcher, Gwern Branwen. This data repository contains scraped webpages from 2013 to 2015. Given the infrequent nature of the scrapes, not all webpages have been collected. Nevertheless, Norbutas (2018) estimates that crawls of Abraxas have successfully collected 92.4% of all listed items on the

Abraxas cryptomarket. This includes information on the vendor name, vendor shipping location, listing title, listing price, listing description, transaction date, buyer unique identifier, buyer rating and buyer feedback. HTML links in the dataset were stitched together in Python to recreate the Abraxas website. This recreated website serves as a copy of the original Abraxas cryptomarket, with information on transactions that were successfully scraped. Furthermore, each webpage in the dataset was manually inspected to identify duplicate transactions based on the feedback provided.

While buyers may leave feedback on their original post, they may also return to alter the message. As such, extracting data from these webpages could yield duplicate transactions if each transaction is not properly inspected. Once all duplicates had been identified and removed, a total of 5434 transactions over a period of 7 months (January to July) in 2015 remained. These were stored in an Excel spreadsheet. While Abraxas was established in December 2014, the first transaction occurred on 15 January 2015. It is important to note that this dataset does not include all recorded transactions on Abraxas. This is due to both the infrequency of the scrapes conducted by Branwen et al. (2015) and the vast number of broken webpages that could not be repaired and accessed. As such, while this dataset includes numbers sufficient for analysis, it does not include the full cohort of transactions on the cryptomarket. This is a clear limitation. Nevertheless, there were 269 unique sellers and 2794 unique buyers in the dataset. Importantly, the Abraxas dataset was previously used by Norbutas (2018) in an examination of the geographical distribution of transactions. For the purposes of this book, a two-mode buyer-seller trade network is reconstructed. These data were used in Chaps. 4 and 5.

This research uses a combination of statistical methods. In Chap. 4, a combination of descriptive network analysis, community detection analysis, statistical modelling and trajectory modelling is utilised. Descriptive statistics were used to summarise market transactions, so as to better understand both the nature and composition of illicit transactions on Abraxas. In contrast, community detection analysis was used to discern the subgroup structure of this transactional criminal network. In addition, three regression models were used to determine the predictors of vendor trustworthiness. Three proxy variables were created to measure vendor trustworthiness: success, popularity and affluence. As trust is manifested in a variety of ways, each of these dependent variables reflects a key element of trust. Finally, this chapter leverages k-means trajectory modelling to examine the developmental pattern of vendor trustworthiness on Abraxas.

Chapter 5 employs sequential node deletion based on six law enforcement strategies: lead k (degree centrality), eccentricity, unique items bought/sold, cumulative reputation score, total purchase price and random targeting. Five outcome variables (number of isolates, number of components, average number of nodes in components, average geodesic distance and number of nodes in the largest component) are used to measure the impact of each targeting strategy. This study sets parameters to govern the purported behaviour of actors when nodes are removed. As such, the transactional network's overall behaviour can be accurately modelled (Bright et al., 2015) using evidence-based calculus.

Conclusion

As with all applied research examining emergent phenomena, this book seeks to provide a more refined understanding of dark web cryptomarkets. More importantly, the following chapters were conceptualised, developed and written with the sole intent of improving present law enforcement strategies which target cryptomarkets. While the results and conclusions drawn from these results are not perfectly generalisable to all cryptomarkets, they aim to provide law enforcement with a better understanding of the dynamics which undergird these markets. More specifically, trust, network structure and the tactical effectiveness of interventions are important considerations in developing more compelling countermeasures against these illicit online marketplaces. For law enforcement to be more effective against cryptomarkets, it is advised that an evidence-based approach be taken.

References

Branwen, G., Christin, N., Décary-Hétu, D., Andersen, R. M., StExo, El Presidente, Anonymous, Lau, D. Sohhlz, Kratunov, D., Cakic, V., Buskirk, V., McKenna, M., & Goode, S. (2015, July 12). *Dark net market archives, 2011–2015*. https://www.gwern.net/DNM-archives

Chiang, S. (2023, September 5). *North Korean hackers have allegedly stolen hundreds of millions in crypto to fund nuclear programs*. CNBC. https://www.cnbc.com/2023/09/06/north-korea-hackers-stole-crypto-to-fund-nuclear-program-trm-chainalysis.html

Curtis, J., & Oxburgh, G. (2022). Understanding cybercrime in 'real world' policing and law enforcement. *The Police Journal, 96*(4), 573–592. https://doi.org/10.1177/0032258X221107584

Décary-Hétu, D., & Giommoni, L. (2017). Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of operation Onymous. *Crime, Law and Social Change, 67*, 55–75.

Dolliver, D. S. (2015). Evaluating drug trafficking on the tor network: Silk road 2, the sequel. *International Journal of Drug Policy, 26*(11), 1113–1123.

Duxbury, S., & Haynie, D. (2017). The network structure of opioid distribution on a darknet cryptomarket. *Journal of Quantitative Criminology, 34*(4), 921–941.

Giommoni, L., Décary-Hétu, D., Berlusconi, G., & Bergeron, A. (2024). Online and offline determinants of drug trafficking across countries via cryptomarkets. In *Crime, law and social change* (pp. 1–25).

Lacey, D., Goode, S., Pawada, J., & Gibson, D. (2020). The application of scam compliance models to investment fraud offending. *Journal of Criminological Research, Policy and Practice, 6*(1), 65–81.

Norbutas, L. (2018). Offline constraints in online drug marketplaces: An exploratory analysis of a cryptomarket trade network. *International Journal of Drug Policy, 56*, 92–100.

Soska, K., & Christin, N. (2015). *Measuring the longitudinal evolution of the online anonymous marketplace ecosystem* [Conference presentation]. 24th USENIX Security Symposium, Washington, D.C.

Tiwari, M., Gepp, A., & Kumar, K. (2020). The future of raising finance-a new opportunity to commit fraud: A review of initial coin offering (ICOs) scams. *Crime, Law and Social Change, 73*, 417–441.

Van Buskirk, J., Bruno, R., Dobbins, T., Breen, C., Burns, L., Naicker, S., & Roxburgh, A. (2017). The recovery of online drug markets following law enforcement and other disruptions. *Drug and Alcohol Dependence, 173*, 159–162.

Chapter 2
Cryptomarkets: History, Structure and Operations

Introduction

The primary objective of this chapter is to synthesise the existing academic literature on cryptomarkets, examining and elucidating various scholarly contributions to this subject. This chapter will serve as a literature review, summarising the findings from peer-reviewed sources and providing a balanced analysis of cryptomarkets grounded in existing research on cybercrime and organised crime as we know them today. This chapter is comprised of five sections. First, the phenomenon of cybercrime is examined, delving into its inception, evolution and organisation. Next, the origins and overall functioning of cryptomarkets are investigated, focusing on the significance of onion routing and cryptocurrencies. The next section analyses the structural characteristics of cryptomarkets. In this analysis, the hierarchical administrative framework of cryptomarkets is examined as well as the mode of governance and the presence of adaptable exchange networks that are deeply ingrained within these markets. Section "Cryptomarket administration" examines the three main aspects of cryptomarket research: the individuals involved, the nations represented and the products made available on these platforms. Section "The who, what and where of cryptomarkets" examines the significance of trust and reputation within cryptomarkets, elucidating the diverse strategies employed by vendors to cultivate trust among buyers. This chapter will establish a solid basis for examining cryptomarket interventions and their subsequent impact on the dark web ecosystem.

V. Harinam, B. Ariel, *Law Enforcement Strategies for Disrupting Cryptomarkets*,
https://doi.org/10.1007/978-3-031-62821-4_2

What Is Cybercrime and How Organised Is It?

The prevalence and complexity of cybercrime activities have surged over the past decade (Phillips et al., 2022). Fraudsters utilising email systems to deceive unsuspecting individuals with fraudulent services and schemes aimed at quick financial gain have been observed for a while (Grabosky, 2007; see more recently Woods & Walter, 2022). Additionally, Internet chatrooms and message boards have been identified as platforms where sexual solicitation occurs, sometimes contributing to the facilitation of the global sex trade (Kamar et al., 2022; Farley et al., 2013). The utilisation of social media platforms by young individuals to engage in bullying behaviours towards their peers has also been documented (Kee et al., 2022). Furthermore, the advancement of technology has resulted in entirely novel categories of criminal activities (Sinclair et al., 2023). Computer-assisted offences such as distributed denial of service attacks and malicious software have caused significant economic damage. Law enforcement agencies face new challenges in the field of cybercrime daily.

While a universally accepted definition is lacking, it is widely agreed upon by scholars that cybercrime encompasses the use of computer technology or cyberspace to facilitate criminal and deviant activities (Bossler & Holt, 2016, p. 45). Furthermore, Grabosky (2007)—and more recently Goni (2022)—classifies cybercrime based on three conceptual dimensions: the utilisation of computers as a means of committing crimes, the targeting of computers as objects of criminal activity and the involvement of computers as secondary elements in criminal acts. However, this categorisation is lacking in one aspect. Although the classification system establishes conceptual demarcations, it frequently encounters instances of categorical convergence. To this extent, certain cyber-enabled crimes fall into multiple categories in this definition. For instance, botnets are a clandestine assemblage of privately owned computers that have been compromised by malicious software and are operated collectively without the awareness or consent of their owners, typically to disseminate unsolicited spam messages. These are compromised computers that are manipulated from a remote location, so computers serve as both the means and the subject of the offence (Ianelli & Hackworth, 2005). Thus, defining cybercrime is not as straightforward as for other crime categories such as homicide, burglary or drug-related offences.

Another type of categorisation was offered by Wall (2001), who identified four distinct types of cybercrime: cyber-trespass, cyber-deception, cyber-pornography and cyber-violence. Similar to the act of trespassing in a physical context, cyber-trespass refers to the unauthorised access of a computer system without the explicit consent of its owner. Cyber-deception, the second category, pertains to the illicit utilisation of the Internet to acquire information from individuals or organisations. Significantly, the concepts of cyber-trespass and cyber-deception are intrinsically connected to the practice of hacking. Holt and Bossler (2014) stated that hackers create viruses and botnet codes, instigating automated malicious attacks. They may also actively participate in attacks against computer systems and sensitive networks

(p. 22). The authors argued that hackers should be primarily understood within the framework of criminality and deviance. In contrast, Brewer and Goldsmith (2014) sought to establish hackers' moral and legal adaptability by proposing the concept of *digital drift*. According to the authors, technological advancements have allowed individuals to engage in criminal activities and lifestyles both online and offline (p. 113). Hackers do not consistently engage in illegal activities; instead, they alternate between intermittent periods of engaging in cybercriminal behaviour and adhering to legal norms.

According to Wall (2007), the third category, known as cyber-pornography, pertains to the various forms of sexual expression facilitated by computer-mediated communications and the dissemination of sexually explicit materials through online platforms (p. 32). This category is widely regarded as the most contentious among the four. Online pornography does not inherently constitute an illegal endeavour in most countries, although it has more content than it should (Lewczuk et al. 2021; Lim et al., 2016; however, compare Strossen, 2000) and is strictly controlled given its addictive nature (see de Alarcón et al., 2019). Cyber-pornography is a prominent component of the Internet, accounting for a substantial share of online data transmission. Many are also concerned about the accessibility and consumption of pornography by minors (Carnevali et al., 2022; Livingstone & Helsper, 2010). Cyber-enabled child pornography, revenge pornography and sexual exploitation are offences that are appropriately classified within this category and are considered crimes in most jurisdictions around the globe.

Cyber-violence constitutes the fourth category within Wall's (2001) comprehensive typology of cybercrime. This pertains to behaviours enacted by individuals that cause harm to others in both virtual and physical environments. This typically encompasses cyberstalking, online harassment and cyberbullying (Dooley et al., 2009; Evangelio et al., 2022; Tokunaga, 2010; Wolak et al., 2007). However, there is a significant conceptual issue with this category (for a broader discussion, Olweus & Limber, 2018). Specifically, "violence" does not fully encompass the descriptive nature of offences in this category. In a more precise manner, while violence generally encompasses physical actions resulting in bodily harm, online stalking, harassment and bullying do not inherently involve physical acts. These criminal activities occur in the virtual realm and do not entail physical damage inflicted upon the victim—unless the online and offline worlds intersect. Thus, again, the dynamic nature of cybercrime results in the gradual obsolescence of definitions and categorisations as time progresses.

Distinct Features of Cybercrime

The larger discourse regarding the novelty of cybercrime is of the utmost significance. The question at hand is whether the concept can be characterised as "old wine in new bottles" or "new wine in new bottles" (Grabosky & Smith, 2001; Wall, 2007; Yar, 2005). In other words, can cybercrimes be considered terrestrial crimes

that have been transformed, or do they represent a distinct manifestation realised through a different modality? Many criminologists argue that a crime is a crime, and the modern modus operandi through which crime is manifested does not necessitate a new set of theories to explain criminal behaviour. Deterrence theory, routine activities theory and opportunity theory can all be used to define deviancy, offline or online. As a result, Grabosky (2007) believed that the nature of crimes committed in cyberspace is similar to that of crimes committed in a physical environment. To clarify, as with its terrestrial counterparts, the occurrence of cybercrime can be understood through the convergence of three essential elements: a vulnerable target, a perpetrator driven by motivations and the absence of an effective guardian. This is the essence of the routine activities theory of crime proposed by Cohen and Felson (1979), which is applied extensively in the area of cybercrime (e.g., Holt & Bossler, 2008; Leukfeldt & Yar, 2016; Williams et al., 2019).

However, Yar (2005, p. 424) presented a counterargument against applying routine activities theory to cybercrime: There is a notable distinction between the organisation of people, objects and activities in the physical world and their arrangement in the virtual world. These elements are typically within the stable and structured spatiotemporal configurations of the physical world, and their organisation becomes less stable in the virtual world. Therefore, applying the principles of routine activities theory to cybercrime is challenging. Multiple features of present-day cybercrime set it apart from street offending; some of these characteristics are offered below.

Transnationality

One distinguishing feature that sets digital criminality apart from criminality in the physical world is the capacity for transnational misconduct. A significant proportion of cybercrimes can occur within a particular jurisdiction despite being instigated in a different jurisdiction. This situation can give rise to substantial complexities when there are variations in laws and priorities across the jurisdictions involved. Suppose an individual from one nation becomes a target of an online investment scam originating in another nation. In that case, it is possible that one, both or neither of the authorities in the respective countries may possess an investigative or punitive interest (for a broader discussion on the globalised nature of cybercrime, see Chen et al., 2023; Lusthaus, 2012; Siregar & Sinaga, 2021), which contributes to the emergence of complex multinational organisations that are based in local areas but have a global reach. Significantly, the utilisation of technology plays a role in restructuring conventional labour divisions within a criminal enterprise that crosses borders. Indeed, artificial intelligence contributes to the automation and reduction of skill requirements in certain illegal activities (for an example in the area of pay-for ransomware services, see Gray et al. 2022), but it also facilitates the acquisition of new skills and enables individuals and groups to engage in criminal enterprises on a global scale (Pease, 1991, p. 24; Savona & Mignone, 2004; Wall, 2007).