THE UNIVERSITY of EDINBURGH
Edinburgh Law School

POSTGRADUATE LAW COURSE ASSESSMENT COVER SHEET

Instructions for students:

Please ensure you have read the formatting and submission guidance available in the Programme Handbook. Unless stated otherwise in the course guidebook, the deadline for submission is 2pm.

1. Please complete the grey shaded areas below.

2. This coversheet must be attached as the first page of your work. No further information is required. Page 2 thereafter, will be the first page of your assessment.

3. When you save and upload your work for submission, you must use the naming convention as laid out in the Programme Handbook. Exam Numbers ensure student anonymity when marking; UUNs and other personal identifiers cannot be used. Failure to follow the naming convention could mean your assessment is not accepted, and penalties may occur.

EXAM NUMBER:	B205697
COURSE CODE:	LAWS11396
QUESTION NUMBER:	2
WORD COUNT:	2497

What, if anything, can be done to combat effectively the sale of illegal goods on 'crypto-markets' on the Darknet?

1. Introduction

Cryptomarkets are online marketplaces located on the darknet, facilitating the sale of illegal goods such as firearms, stolen credentials, and drugs. Anonymous payment methods, ease of accessibility and less transactional violence are a few reasons individuals may choose to buy these goods online. In addition, these marketplaces deploy similar tactics to legitimate businesses, such as allowing customers to leave reviews and creating a user-friendly online shopping layout similar to eBay (Christin, 2013). Operations undertaken by law enforcement organisations to reduce the sale of illegal goods on the darknet have previously been challenging and, in some cases, have had the adverse effect of causing more transactions to occur (Tsuchiya & Hiramoto, 2021). Approaches taken by law enforcement have resulted in limited success and international agencies have called for a deeper understanding of cryptomarkets (Décary-Hétu & Giommoni, 2017). The lack of collaboration between law enforcement agencies can also be detrimental to the success of takedown operations as illegal goods on cryptomarkets are sold across the globe (Barratt & Aldridge, 2020).

This paper portrays the overall argument that increasing global collaboration amongst law enforcement organisations and leveraging crime scripts when planning targeted takedown operations could be practical approaches to reduce the sale of illegal goods on the darknet.

The structure of the paper is as follows. Section 1 introduces the topic and the argument presented. Section 2 provides background knowledge regarding Tor, cryptomarkets and crime scripts. Section 3 examines the challenges law enforcement can face when tackling cryptomarket sales. Section 4 explores the need for global collaboration to improve law enforcement operations. Section 5 suggests using crime scripts to develop a more targeted and creative approach for law enforcement operations. Section 6 provides a conclusion to the argument presented.

2. Background Knowledge

2.1 Tor

The Tor network is an encrypted system that can function as a network of virtual tunnels to ensure secure communication and improve privacy on the internet. An examination of users' engagement on Tor, indicates only 6.7% of users engage with 'Onion/Hidden services' on an average day, which are generally used for illegal activity (Jardine, Lindner & Owenson, 2020). Despite this small percentage, the internet browser can facilitate the sale of illegal goods anonymously on a global scale and has consistently overcome takedown methods, such as the blockage of Tor relays by China (Chertoff, 2017).

2.2 Cryptomarkets

Cryptomarkets leverage the concealed hosting capabilities of Tor providing a platform to exchange illegal goods. Barratt and Aldridge (2016) defines cryptomarkets as a marketplace with multiple suppliers and buyers, enabling users' anonymity via cryptocurrencies as a payment method. Cryptomarkets can be accessed through the darknet: a layer of the internet, hosting websites intentionally concealed from the public and only accessible through specific software utilising decentralised and anonymised nodes such as Tor (Finklea, 2017). Once on the Tor network, users may be able to locate cryptomarkets through dark web search engines. However Weimann (2016) indicated that they are limited in scope and usefulness and despite recent advancements in these tools, users could still use blogs and websites to search for the 16-digit onion addresses, needed to access cryptomarkets.

2.3 Overview of Crime Scripts

Crime scripts create an in-depth understanding of the necessary steps and actions a user would undertake to prepare for, perform and commit a crime (Holt & Lee, 2022b). Cornish (1994) introduced this script-theoretic approach and claims knowledge generated by crime scripts can enhance situational crime prevention policies and highlight possible intervention points. Dehghanniti and Borrion have praised Cornish's approach as 'seminal' (2021, p.505) and a 'methodical landmark' (2021, p.518), as it has become increasingly popular over the last twenty years. Crime scripts which have been created for cybercrimes, fraud, and robbery have previously been successful, and recommendations have been made to use crime scripts to tackle broader problems (Dehghanniri & Borrion, 2021).

3. Challenges Law Enforcement Face

3.1 Failure of Traditional Methods

Police operations that follow blanket approaches, such as using traditional offline methods to tackle the sale of drugs on cryptomarkets, have previously been deemed ineffective by both academics and law enforcement officials (Décary-Hétu & Giommoni, 2017; Minnaar, 2017). Combining this knowledge with the increased improvement of privacy tools and cryptocurrency anonymity, suggests that law enforcement can struggle to identify individuals who use cryptomarkets. Detailed research on criminal markets, both online and offline, reveals their resistance to intervention and their quick recovery in the face of legal actions (Masson & Bancroft, 2018). Since 66.1% of cryptomarket users tend to migrate from a blocked market to the next largest open marketplace, strategies to enhance law enforcement takedown operations must be created (Elbahrawy et al., 2020).

3.2 Impact of Media Attention

Data shows that the search term ‘dark web’ drastically increased on Google from 2014 to 2019 (Jardine, 2021). The impact of the police takedown labelled ‘Operation Onymous’ may be the reason for this increase due to the substantial amount of media attention received after seizures occurred (Tsuchiya & Hiramoto, 2021). Since the operation attracted significant public attention, an idea can be presented that it may have informed the public of the capabilities of the darknet, thus spurting growth in the number of users of cryptomarkets.

3.3 Modern Delivery Mechanisms

When sending drugs, vendors tend to package their goods using stealth shipping techniques (Rhumorbarbe et al., 2016), resulting in fewer packages being intercepted by law enforcement. Décary-Hétu et al. (2016) shows that the willingness of cryptomarket vendors to ship internationally is based on package size and the perceived effectiveness of law enforcement in the destination country. Dropshipping is an alternative method for vendors to send their products without even possessing the goods themselves. This framework involves using a third party as a delivery service, which may disrupt police investigations. Aldridge and Askew (2017) claimed it is currently unclear if this tactic is being deployed on cryptomarkets to provide an additional security layer to vendors, however, due to the rise in dropshipping popularity, it may be likely (Singh, Kaur & Singh, 2018).

3.4 Advanced Payment Methods

Bitcoin is the standard payment choice on cryptomarkets, as it is can be viewed as one of the world's most well-known cryptocurrencies. However, the cryptocurrency Monero has recently increased in popularity as it deploys different cryptographic algorithms which group transactions together on the blockchain, thus making it harder to identify individuals. Furthermore, the ability of law enforcement to discover buyers and sellers identities using blockchain analysis, which was becoming increasingly successful on Bitcoin, has been severely limited when users are switching to Monero (Hardeveld et al., 2017; Horton-Eddison et al., 2021). This may be the reason more users are adopting it, as it could be viewed as the optimal payment method for users, to preserve their anonymity.

4. Global Collaboration

4.1 Benefits of Global Cooperation

Increasing international cooperation can have huge benefits as it allows law enforcement to gain access to better resources and tools while leveraging skillsets from across the world in their fight against the darknet. According to the Stanford Law Review, around 80% of the machines on the dark web are hosted outside of the United States (Ghappour, 2017). Therefore, the geographical location of a darknet server can become particularly disruptive during law enforcement investigations since the servers may be in countries where international relations are weak, resulting in minimal cooperation and support. A criminal may even leverage this weakness and choose to host their server within a country with fragile international relations to avoid facing prosecution.

However, law enforcement operations which target cryptomarkets hosted on these servers or hosted at data centres across the globe could be less challenging to takedown, due to the cross-jurisdictional approaches a formal international agreement would allow. With global support, strategies to enhance the takedown of these cryptomarkets could involve obtaining local government assistance or help from cloud service providers to leverage their knowledge when classifying data belonging to a suspect (Hardeveld et al., 2017).

4.2 Lack of Guidance

Despite repeated requests by officials for comprehensive international guidance regarding drug cryptomarkets, no such approach has been developed. Instead, limited documentation has been issued to countries on cryptomarkets, and pieces of critical information have been displaced across multiple United Nations statements and resolutions (Horton-Eddison et al., 2021). The distribution of this information could make it difficult for countries to comply with requests for global cooperation, especially since these requests seem generic and can lack in detail (Horton-Eddison et al., 2021). A speech given by the General Director of the United Nations Office on Drugs and Crime explains the “importance of coordinated action” and the need to “strengthen international cooperation” to tackle the growth of cryptomarkets (United Nations Office on Drugs and Crime, 2018). Additionally, Interpol has commented on the need for an official international strategy to prevent illegal cryptomarket transactions from occurring (Europol, 2021).

Although some informal global agreements may have taken place during joint operations, no official legally binding policy has been created. This could result in international disputes during investigations, potentially worsening the global communication problem (Wang et al., 2022). There is a gap in the literature regarding why no formal international strategy exists; however, perhaps global politics and relations between countries would be influencing factors here.

4.3 Unlawful Network Access

The use of hacking techniques by law enforcement has been deployed in the past to takedown cryptomarkets even though it may violate the sovereignty of other nations (Williams, 2017). Ghappour (2017) presents the idea that criminal procedure should be amended to prevent network investigations from ruining international relations and limiting political fallouts. However, a contrasting viewpoint could be presented that an increase in global collaboration should be the priority since it can reduce the occurrence of unlawful network access rather than mitigating the impact, after the fact.

5. Crime Scripts

5.1 Crime Scripts for Cryptomarkets

Multiple crime scripts have previously been created to analyse the sale a specific illegal good on the cryptomarkets. Holt and Lee (2020) have examined the sale of counterfeit identification documents, Jardine (2021) analysed drug sales and Holt and Lee (2022) then explored the sale of weapons. These scripts allow each of the steps taken by individuals to buy or sell an item on cryptomarkets to be categorised, enabling law enforcement to explore numerous intervention opportunities (Hutchings & Holt, 2015). Since crime scripts do not need to have a defined approach (Cornish, 1994), a claim by Jardine (2021) indicates that all crime scripts developed for cryptomarkets can consist of the following four stages: information gathering; account creation; use of the marketplace and delivery/receipt. An analysis of literature confirms this classification as acceptable as research shows multiple crime scripts in this area follow a similar structure (Holt & Lee, 2022a, 2022b; Hutchings & Holt, 2015; Warren et al., 2017).

5.2 Using Crime Scripts in Law Enforcement

As argued in Section 3.1, blanket techniques for operations by law enforcement can have little success. Therefore this paper suggests that operations should target their takedown operations based on a crime script, using the four stages identified by Jardine (2021). Section 5.2.1 - 5.2.4 explains each of these stages and details examples of how previous police operations may have unintentionally proven the success of using a targetted approach during their operations.

5.2.1 Information Gathering

For an individual to buy/sell illegal goods on the darknet, logically, they first must gather information regarding what the darknet is, how they can access it through Tor, and discover onion addresses of active cryptomarkets. Jardine (2021) proposes that law enforcement should use either an investegory apporach, such as examining the digital traces left by darknet users or a preventative approach, such as reducing information for accessing cryptomarkets since this has previously played a considerable role in the growth of cryptomarket sales (Décary-Hétu & Giommoni, 2017). A unique example of using information gathering techniques can be seen in ‘Operation Marco Polo’ in 2013, however the success of this operation seems to have relied on mistakes made by the criminals (Minnaar, 2017).

5.2.2 Account Creation

Once users have gathered enough information and downloaded all required tools, such as Tor, they would likely create a cryptocurrency wallet for a payment method and register for an account on an illegal marketplace. Law enforcement may target this stage by attempting to take over control over a marketplace rather than shut it down, allowing them to perform various investigatory tasks such as modifying the code to record a user's details when registering for an account. This tactic was deployed in ‘Operation Bayonet/GraveSac’ in 2018 however, this joint investigation was not planned, and it could be deemed a coincidence that one law enforcement organisation had what another needed without any prior planning or collaboration (Jardine, 2021).

5.2.3 Marketplace Use

Law enforcement can leverage marketplace use by performing methods such as posing as a buyer, seller, or admin to deanonymise individuals on cryptomarkets. For example, ‘Operation Hyperion’ also undertaken in 2018, used the marketplace as a contact tool to approach users who were suspected of drug trading and warn them that they have been observed committing crimes. This action sparked multiple worried discussions on Reddit, indicating users were indeed impacted by it, even if the outcome of this impact was challenging to measure (Bradley & Stringhini, 2019).

5.2.4 Delivery/Receipt

Sellers and buyers face the challenge of either transporting or obtaining their goods purchased/sold on cryptomarkets without detection. Law enforcement could adopt multiple methods to intercept packages in this stage and undertake controlled deliveries in an attempt to convict drug buyers with intent to supply (Matthews et al., 2020). ‘Operation Disrupt Tor’ was one of the first law enforcement attempts to consistently follow a targeted approach using global collaberation throughout their operations. This investigation focused on the delivery/recipient stage of this suggested crimescript and was deemed highly successful, facilitating the arrests of 179 individuals across seven countries (United States Department of Justice, 2022). This operation showcases what global orginisations could achieve in each stage of the crime script process if they were to consider new takedown ideas and undertake an offical global collaberitive apporach.

6. Conclusion

This paper suggests that police operations have had a limited impact in preventing the sale of illegal goods on cryptomarkets due to the lack of global collaboration and targeted approaches. Our analysis shows that operations which target the series of steps involved in the purchase/sale of illegal goods have been more effective than using a blanket level approach. However, these successful operations undertaken by law enforcement lack structure as they rely on luck derived from other operations, criminals' mistakes, and other coincidental factors. The use of crime scripts in law enforcement operations would provide a framework to efficiently plan better-targeted takedown approaches by examining all actions individuals undertake when buying/selling illegal goods on cryptomarkets. The need for global collaboration in this field has also never been higher, as cryptomarket users may currently leverage this weakness to transfer goods across borders, recruit more users and remain undetected. Deploying a formal international collaboration strategy would combat this, and allow takedown operations to run more smoothly, operate more efficiently and apprehend more criminals.

References

Aldridge, J. & Askew, R. (2017) Delivery dilemmas: How drug cryptomarket users identify and seek to reduce their risk of detection by law enforcement. *The International journal on drug policy*. 41, 101–109.

Barratt, M.J. & Aldridge, J. (2016) Everything you always wanted to know about drug cryptomarkets* (*but were afraid to ask). *International Journal of Drug Policy*. 35, 1–6. doi:10.1016/J.DRUGPO.2016.07.005.

Barratt, M.J. & Aldridge, J. (2020) No magic pocket: Buying and selling on drug cryptomarkets in response to the COVID-19 pandemic and social restrictions. *The International journal on drug policy*. 83. doi:10.1016/J.DRUGPO.2020.102894.

Bradley, C. & Stringhini, G. (2019) A Qualitative evaluation of two different law enforcement approaches on dark net markets. In: *2019 EEE European Symposium on Security and Privacy Workshops*. 1 June 2019 Stockholm, Institute of Electrical and Electronics Engineers Inc. pp. 453–463. doi:10.1109/EUROSPW.2019.00057.

Chertoff, M. (2017) A public policy perspective of the Dark Web. *Journal of Cyber Policy*. 2 (1), 26–38. doi:10.1080/23738871.2017.1298643.

Christin, N. (2013) Traveling the silk road: a measurement analysis of a large anonymous online marketplace. In: *WWW '13: Proceedings of the 22nd international conference on World Wide Web*. 2013 Brazil, Association for Computing Machinery. pp. 213–224. doi:10.1145/2488388.2488408.

Cornish, D. (1994) *The Procedural Analysis of Offending and its Relevance for Situational Prevention*. London, Criminal Justice Press.

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 (1), 55–75. doi:10.1007/s10611-016-9644-4.

Décary-Hétu, D., Paquet-Clouston, M. & Aldridge, J. (2016) Going international? Risk taking by cryptomarket drug vendors. *International Journal of Drug Policy*. 35, 69–76. doi:10.1016/J.DRUGPO.2016.06.003.

Dehghanniri, H. & Borrion, H. (2021) Crime scripting: A systematic review: *European Journal of Criminology*. 18 (4), 504–525. doi:10.1177/1477370819850943.

Elbahrawy, A., Alessandretti, L., Rusnac, L., Goldsmith, D., Teytelboym, A. & Baronchelli, A. (2020) Collective dynamics of dark web marketplaces. *Sci Rep 10 18827*.10. doi:10.1038/s41598-020-74416-y.

Europol (2021) *Internet Organised Crime Threat Assessment (IOCTA) 2021*. Luxembourg, Publications Office of the European Union. doi:10.2813/113799.

Finklea, K. (2017) *Dark Web*. 2017. Congressional Research Service. https://sgp.fas.org/crs/misc/R44101.pdf [Accessed: 23 April 2022].

Ghappour, A. (2017) *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*. 2017. 69 Stanford Law Review 1075. https://scholarship.law.bu.edu/faculty_scholarship/204 [Accessed: 25 April 2022].

Hardeveld, J. Van, Jan, G., Webber, C. & O'hara, K. (2017) Deviating From the Cybercriminal Script: Exploring Tools of Anonymity (Mis)Used by Carders on Cryptomarkets. *American Behavioral Scientist*. 61 (11), 1244–1266. doi:10.1177/0002764217734271.

Holt, T.J. & Lee, J.R. (2022a) A Crime Script Analysis of Counterfeit Identity Document Procurement Online. *Deviant Behavior*. 43 (3), 285–302. doi:10.1080/01639625.2020.1825915.

Holt, T.J. & Lee, J.R. (2022b) A crime script model of Dark web Firearms Purchasing. *American Journal of Criminal Justice*. doi:10.1007/S12103-022-09675-8.

Horton-Eddison, M., Shortis, P., Aldridge, J. & Caudevilla, F. (2021) *Drug Cryptomarkets in the 2020s: Policy, Enforcement, Harm, and Resilience*. Swansea, Global Drug Policy Observatory and University of Manchester.

Hutchings, A. & Holt, T.J. (2015) A Crime Script Analysis of the Online Stolen Data Market. *The British Journal of Criminology*. 55 (3), 596–614. doi:10.1093/bjc/azu106.

Jardine, E. (2021) Policing the Cybercrime Script of Darknet Drug Markets: Methods of Effective Law Enforcement Intervention. *American Journal of Criminal Justice*. 46 (6), 980–1005. doi:10.1007/s12103-021-09656-3.

Jardine, E., Lindner, A.M. & Owenson, G. (2020) The potential harms of the Tor anonymity network cluster disproportionately in free countries. *Proceedings of the National Academy of Sciences*. 117 (50), 31716–31721. doi:10.1073/pnas.2011893117.

Masson, K. & Bancroft, A. (2018) 'Nice people doing shady things': Drugs and the morality of exchange in the darknet cryptomarkets. *International Journal of Drug Policy*. 58, 78–84. doi:10.1016/J.DRUGPO.2018.05.008.

Matthews, B., McVie, S., Dibben, C. & Collier, B. (2020) *Postal Delivery of Illegal Consignments into Scotland: Dataset Description*. Elsevier BV. doi:10.2139/SSRN.3611823.

Minnaar, A. (2017) Online 'Underground' Marketplace for Illicit Drugs : The Prototype Case of the DarkWeb Website 'Silk Road'. *Acta Criminologia : Southern African Journal of Criminology*. 30 (1), 23–47.

Rhumorbarbe, D., Staehli, L., Broséus, J., Rossy, Q. & Esseiva, P. (2016) Buying drugs on a Darknet market: A better deal? Studying the online illicit drug market through the analysis of digital, physical and chemical data. *Forensic Science International*. 267, 173–182. doi:10.1016/J.FORSCIINT.2016.08.032.

Singh, G., Kaur, H. & Singh, A. (2018) *Dropshipping in E-Commerce: A Perspective*. 2018. ICEME 2018: Proceedings of the 2018 9th International Conference on E-business, Management and Economics. doi:10.1145/3271972.3271993 [Accessed: 25 April 2022].

Tsuchiya, Y. & Hiramoto, N. (2021) Dark web in the dark: Investigating when transactions take place on cryptomarkets. *Forensic Science International: Digital Investigation*. 36, 301093. doi:10.1016/J.FSIDI.2020.301093.

United Nations Office on Drugs and Crime (2018) *Remarks at the launch of the World Drug Report 2018*. 2018. https://www.unodc.org/unodc/en/speeches/2018/wdr18-260618.html [Accessed: 24 April 2022].

United States Department of Justice (2022) *International Law Enforcement Operation Targeting Opioid Traffickers on the Darknet Results in over 170 Arrests Worldwide and the Seizure of Weapons, Drugs and over $6.5 Million*. 22 September 2022. DOJ Office of Public Affairs. https://www.justice.gov/opa/pr/international-law-enforcement-operation-targeting-opioid-traffickers-darknet-results-over-170 [Accessed: 25 April 2022].

Wang, C., Lassi, N., Zhang, X. & Sharma, V. (2022) The Evolving Regulatory Landscape for Fentanyl: China, India, and Global Drug Governance. *International journal of environmental research and public health*. 19 (4). doi:10.3390/ijerph19042074.

Warren, S., Oxburgh, G., Briggs, P. & Wall, D. (2017) How might crime-scripts be used to support the understanding and policing of cloud crime? In: *International Conference on Human Aspects of Information Security, Privacy, and Trust*. 2017 Springer Verlag. pp. 539–556. doi:doi.org/10.1007/978-3-319-58460-7.

Weimann, G. (2016) Terrorist Migration to the Dark Web. *Perspectives on Terrorism*. 10 (3), 40–44.

Williams, W. (2017) The Race for Privacy: Technological Evolution Outpacing Judicial Interpretations of the Fourth Amendment: Playpen, the Dark Web, and Governmental Hacking. *Florida State University Law Review*. 45 (1), 1211–1240.